

Rec'd PCT/PTO 24 JUN 2005
PCT/JPO3/16737

日 本 国 特 許 庁
JAPAN PATENT OFFICE

10/540768
25.12.03

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: 2 0 0 2 年 1 2 月 2 5 日

出 願 番 号
Application Number: 特 願 2 0 0 2 - 3 7 5 1 2 3
[ST. 10/C]: [J P 2 0 0 2 - 3 7 5 1 2 3]

REC'D 19 FEB 2004

WIPO

PCT

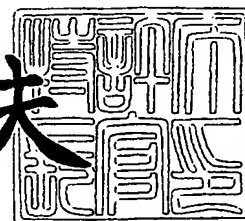
出 願 人
Applicant(s): 株式会社日立製作所

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

2 0 0 4 年 2 月 5 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



【書類名】 特許願

【整理番号】 HK14713000

【提出日】 平成14年12月25日

【あて先】 特許庁長官 殿

【国際特許分類】 H04L 9/16

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所 システム開発研究所内

【氏名】 水谷 美加

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所 システム開発研究所内

【氏名】 神牧 秀樹

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所 システム開発研究所内

【氏名】 海老名 明弘

【特許出願人】

【識別番号】 000005108

【氏名又は名称】 株式会社 日立製作所

【代理人】

【識別番号】 100084032

【弁理士】

【氏名又は名称】 三品 岩男

【電話番号】 045(316)3711

【手数料の表示】

【予納台帳番号】 011992

【納付金額】 21,000円

【提出物件の目録】

【物件名】	明細書	1
【物件名】	図面	1
【物件名】	要約書	1
【プルーフの要否】	要	

【書類名】 明細書

【発明の名称】 ネットワーク機器、ネットワークシステム、および、グループ管理方法

【特許請求の範囲】

【請求項 1】

ネットワークを介して接続された他のネットワーク機器と通信を行なうネットワーク機器であって、

互いに認証可能な前記ネットワーク機器をグループとして管理するグループ管理手段と、

前記グループ所属するネットワーク機器間で共通の暗号化鍵による暗号通信を行う暗号通信手段と、

前記暗号化鍵の情報と前記グループに所属するネットワーク機器のホスト名およびアドレスを含む識別情報とを含む、前記グループに所属するネットワーク機器と暗号通信を行うために必要な暗号通信情報を格納する記憶手段と、

外部から情報を取得する取得手段と、を備え、

前記グループ管理手段は、

前記記憶手段に前記暗号通信情報が格納されていない状態で、前記取得手段において前記暗号通信情報を取得すると、当該暗号通信情報を前記記憶手段に格納するとともに、前記暗号通信手段を介して自身の識別情報を前記グループに所属するネットワーク機器に送信し、

前記暗号通信手段を介して他のネットワーク機器から当該他のネットワーク機器の識別情報を取得すると、前記記憶手段に記憶している前記暗号通信情報に当該識別情報を追加する

ことを特徴とするネットワーク機器。

【請求項 2】

請求項 1 記載のネットワーク機器であって、

前記グループ管理手段は、さらに、

前記取得手段においてグループから離脱する指示を受け付けると、前記記憶手段に記憶されている前記グループに所属する全てのネットワーク機器に、前記暗

号通信手段を介して自身のネットワーク機器の離脱を通知するとともに、前記記憶手段から前記暗号通信情報を削除し、

前記暗号通信手段を介して他のネットワーク機器から、当該他のネットワーク機器が離脱する通知を受け付けると、前記記憶手段に記憶している前記暗号通信情報から、当該他のネットワーク機器の識別情報を削除する、

ことを特徴とするネットワーク機器。

【請求項 3】

請求項 1 または 2 記載のネットワーク機器であって、

前記取得手段は、記憶媒体のインタフェースであり、

前記グループ管理手段は、さらに、

前記記憶手段に前記暗号通信情報が格納されている状態で、前記暗号通信情報が格納された記憶媒体が前記取得手段に挿入された場合、前記記憶手段に格納されている暗号通信情報を前記記憶媒体にコピーすること

を特徴とするネットワーク機器。

【請求項 4】

請求項 1、2、または、3 記載のネットワーク機器であって、

非暗号通信を行なう非暗号通信手段と、

前記ネットワーク機器が提供するサービスに対するアクセスを制御するアクセス制御手段とをさらに備え、

前記アクセス制御手段は、前記非暗号通信手段を介して他のネットワーク機器からアクセスがあった場合、前記アクセスが予め定められたポートに対するものである場合、前記アクセスを許可すること

を特徴とするネットワーク機器。

【請求項 5】

複数のネットワーク機器と、前記複数のネットワーク機器を接続するネットワークとを備えたネットワークシステムにおいて、

前記複数のネットワーク機器は、請求項 1～4 記載のネットワーク機器であることを特徴とするネットワークシステム。

【請求項 6】

ネットワークを介して接続された他の機器と、互いに認証可能な暗号通信を行なうグループを管理するグループ管理方法であって、

前記ネットワークに接続された一つの機器において、前記暗号通信に用いる暗号化鍵を生成し、当該暗号化鍵と自機器のホスト名とアドレスとを含む識別情報とを暗号通信情報として保有するグループ生成ステップと、

前記暗号通信情報を取得した機器において、前記暗号通信情報に前記識別情報が格納されている全機器に自身の識別情報と参加を示す情報とを前記暗号通信により通知し、当該暗号通信情報に自身の識別情報を追加して保有する第 1 のグループ参加ステップと、

当該識別情報と前記参加を示す情報とを受けた機器において、自身が保有する前記暗号通信情報に当該識別情報を追加する第 2 のグループ参加ステップと、

前記グループから離脱する指示を受け付けた機器において、自身を除く前記暗号通信情報に前記識別情報が格納されている全機器に離脱を示す情報と自身の識別情報とを前記暗号通信により通知し、自身の保有する前記暗号通信情報を削除する第 1 のグループ離脱ステップと、

当該離脱の通知を受けた機器において、自身が保有する前記暗号通信情報から通知を受けた識別情報を削除する第 2 のグループ離脱ステップと、

を備えることを特徴とするグループ管理方法。

【請求項 7】

コンピュータを、

暗号通信に用いる暗号化鍵を生成し、当該暗号化鍵と自身のホスト名およびアドレスを含む識別情報とを暗号通信情報として保有するグループ生成手段と、

前記暗号通信情報を取得すると、前記暗号通信情報に前記識別情報が格納されている全機器に自身の識別情報と参加を示す情報とを前記暗号通信により通知し、前記暗号通信情報に前記自身の識別情報を追加して保有する第 1 のグループ参加手段と、

他の機器から当該機器の識別情報と参加を示す情報とを受信すると、自身が保有する前記暗号通信情報に当該識別情報を追加する第 2 のグループ参加手段と、

前記暗号通信情報を削除する指示を受け付けると、自身を除く前記暗号通信情

報に前記識別情報が格納されている全機器に離脱を示す情報と前記自身の識別情報とを前記暗号通信により通知し、自身の保有する前記暗号通信情報を削除する第 1 のグループ離脱手段と、

他の機器の識別情報と前記離脱を示す情報とを受信すると、自身が保有する前記暗号通信情報から受信した識別情報を削除する第 2 のグループ離脱手段、
として機能させるためのプログラム。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、ネットワークに接続する特定の機器間で排他的かつ安全に通信を行う技術に関する。

【0 0 0 2】

【従来の技術】

Internet Protocol（以下、I P と呼ぶ）と呼ばれる通信プロトコルを使用する I P ネットワークは、コンピュータネットワークのデファクトスタンダードとしての地位を確立し、一般ユーザへの普及が著しい。

【0 0 0 3】

この I P ネットワークを介して機器間でデータをやりとりするには、その機器それぞれに一意的に I P アドレスを付与することが必要である。現在では、I P アドレスを 3 2 ビットで表す I P v 4 (Internet Protocol version 4) が用いられているが、I P ネットワークの利用が増大するに連れて、I P アドレスの不足が大きな問題となってきた。

【0 0 0 4】

このような状況を背景に、I P アドレスを 1 2 8 ビットに拡張し、さらに、セキュリティ機能など、今までの I P アドレスになかった機能を付加した新しい I P アドレスを用いる I P ネットワークとして I P v 6 (Internet Protocol version 6) が I E T F (Internet Engineering Task Force) にて採択され、それを用いたネットワークサービスが次世代 I P として標準化されつつある。

【0 0 0 5】

さらに、使用可能なアドレス数が増え、セキュリティ機能が充実した I P v 6 の新たな適用先として、冷蔵庫、洗濯機などの白物家電、あるいはテレビ、ビデオといったAV機器といった家庭内の機器から構成されるホームネットワークなどが注目されている。

【 0 0 0 6 】

これらの機器それぞれに I P アドレス割り当てることにより、各機器をサーバとみなすことができるようになり、機器間通信により新しいサービスを実現したり、外部端末からの機器の制御、サービスセンタからの機器の制御といったインターネットを介した新しいサービスを実現するといったことが考えられている。

【 0 0 0 7 】

ところで、家庭内機器のような特定の機器間の通信においては、利用者が認識している範囲外の機器からの操作を排除するようなシステムが要求される。例えば、友人が持ってきた機器による勝手な操作の防止が必要である。

【 0 0 0 8 】

すなわち、利用者が互いの通信を許可する範囲を決定し、それらの機器をグループ化し、グループ化された機器間でのみ通信がなされるようなシステムが要求される。そして、このような通信を実現するためには、グループ内の機器間で、互いをグループ内に属する真正な機器であることを認証するための認証機能が必要である。

【 0 0 0 9 】

このような認証機能として、従来のクライアント、サーバ型のシステムでは、認証サーバを用いたものが実現されている。例えば、R F C 2 8 6 5 で定義される R A D I U S (Remote Authentication Dial-In User Service) では、サーバにアクセスするクライアントのアカウント (ユーザ名、パスワード) を R A D I U S サーバと呼ばれる認証サーバで一括管理し、サーバは、クライアントからのアクセス要求 (ユーザ名点パスワードを含む) を R A D I U S サーバに転送しアクセス可否の判断結果を受けて、クライアントとの通信を行うかどうか判断する。

【 0 0 1 0 】

例えば、従来のグループ化された特定の機器間での暗号通信システム及びその

通信方法としては、特開 2002-124941 号公報（特許文献 1）及び特開平 5-347616 号公報（特許文献 2）に示されているものがある。

【特許文献 1】 特開 2002-124941 号公報

【特許文献 2】 特開平 5-347616 号公報

【発明が解決しようとする課題】

ホームネットワークに接続されている機器の中で、利用者が指定した機器間でのみ所定の通信を行うためには、互いに相手が指定された機器であることを認証する機能が必要と考えられている。

【0011】

従来の認証機能は、クライアント・サーバシステムが前提であり、サーバにアクセスするクライアントのアクセス情報を管理する認証サーバを備えることで実現されている。

【0012】

これに対し、ホームネットワークを構成する機器は、適宜サービスに応じて必要な機器間で通信を行なうといったアドホック型である。このため、全ての機器がサーバにもクライアントにもなり得、アクセス情報の設定がより煩雑になるという問題がある。

【0013】

このような場合に、従来のように認証サーバを備え、機器間でのセッション確立毎、あるいはサービス開始毎に個別に認証を行うようにすると、認証のオーバーヘッドが大きくなるという問題もある。

【0014】

例えば、前述の特許文献 1 に開示された技術は、認証機能を有したグループ通信システムである。本技術は、グループを構成する機器以外に、グループ通信システム内にグループ暗号鍵を生成する機能及びグループに所属する端末情報を管理する機能を備えたグループ暗号鍵管理部と及び中継装置とを備えて構成され、大規模なネットワーク構成を前提としたものである。

【0015】

また、前述の特許文献 2 に開示された技術は、まず、グループ通信を行う機器

ごとにＩＣカードを具備していなければならない。そして、そのＩＣカードには、予め送受信相手の所属ごとに設定された複数のマスタ鍵とグループ鍵生成プログラムとが記録されている必要がある。

【0016】

このように、従来の技術では、実際に通信を行なう機器以外に認証サーバとなる機器を用意する必要があったり、マスタ鍵と個々の通信相手先の関係といった複雑な情報を予め記憶させておく記録媒体をグループを構成する機器の数だけ用意する必要があった。

【0017】

本発明は、このような事情に鑑みなされたもので、本発明の目的は、利用者が認めた機器間で容易に互いを認証し合うことが可能なグループを構成し、そのグループに属する機器間の安全な通信を実現することにある。

【0018】

さらに、本発明の他の目的は、グループ内の機器が提供するアプリケーションにグループ外の機器にもアクセスを許可するものがある場合、グループ外の機器から、そのアプリケーションにのみアクセスを許可するといったアクセス制御を実現することにある。

【0019】

【課題を解決するための手段】

本発明は、共有の鍵を用いて暗号通信を行うことで互いを認証し、セキュリティの確保された通信を行なう機器の集まりをグループとみなし、そのグループを構成する機器となりうる個々の機器のいずれもが、グループを生成し、参加し、また、そのグループから離脱するといったグループ管理の手段を有する。

【0020】

また、機器がいずれかのグループに属していても、グループ外の機器との通信の可能性も保有するものである。

【0021】

具体的には、ネットワークを介して接続された他のネットワーク機器と通信を行なうネットワーク機器であって、互いに認証可能な前記ネットワーク機器をグ

ループとして管理するグループ管理手段と、前記グループ所属するネットワーク機器間で共通の暗号化鍵による暗号通信を行う暗号通信手段と、前記グループに所属するネットワーク機器の、ホスト名とアドレスとを含む識別情報および前記暗号化鍵の情報を含む前記グループに所属するネットワーク機器と暗号通信を行うために必要な暗号通信情報を格納する記憶手段と、外部から情報を取得する取得手段と、を備え、前記グループ管理手段は、前記記憶手段に前記暗号通信情報が格納されていない状態で、前記取得手段において前記暗号通信情報を取得すると、当該暗号通信情報を前記記憶手段に格納するとともに、前記暗号通信手段を介して自身の識別情報を前記グループに所属するネットワーク機器に送信し、前記暗号通信手段を介して他のネットワーク機器から当該他のネットワーク機器の識別情報を取得すると、前記記憶手段に記憶している前記暗号通信情報に当該識別情報を追加することを特徴とするネットワーク機器を提供する。

【0022】

また、前記グループ管理手段は、さらに、前記取得手段においてグループから離脱する指示を受け付けると、前記記憶手段に記憶されている前記グループに所属する全てのネットワーク機器に、前記暗号通信手段を介して自身のネットワーク機器の離脱を通知するとともに、前記記憶手段から前記暗号通信情報を削除し、前記暗号通信手段を介して他のネットワーク機器から、当該他のネットワーク機器が離脱する通知を受け付けると、前記記憶手段に記憶している前記暗号通信情報から、当該他のネットワーク機器の識別情報を削除する、ことを特徴とするネットワーク機器を提供する。

【0023】

【発明の実施の形態】

以下、本発明の実施の形態を、図を用いて説明する。

【0024】

本実施形態では、宅内において家電などにより構成されるネットワークに本発明を適用した場合を例にあげ、説明する。

【0025】

本実施形態の宅内のネットワークは、IP v 6により構成され、それぞれに I

Pアドレスが付与された、例えば、電子レンジやエアコンなどの家電機器、テレビやビデオなどのAV機器、センサ等が接続されている。以下、ネットワークに接続され、IPv6によるIPアドレスを付与されている各機器を、ノードと呼ぶこととする。

【0026】

本実施形態では、これらのノードのうち、利用者が互いに通信を行なうことを許可したものをグループとし、グループに属するノード間で認証のために共通の暗号化鍵による暗号通信を行なう。

【0027】

ここで、本ネットワークで採用しているIPv6は、前述したように、確保できるIPアドレス数が莫大となるだけでなく、IPsecと呼ばれる暗号・認証の仕組みが標準で装備され、高度な安全性を保ちながら、使い勝手もよいという特徴を持つ。本実施形態においては、IPv6のIPsecを用いて、グループを構成する機器間のみでの安全な通信を実現する。

【0028】

本実施形態の詳細な説明の前に、まず、IPsecの概要について説明する。IPsecは、IP層において相互接続可能で高品質な暗号化ベースのセキュリティを提供する技術である。このセキュリティは、認証ヘッダAH (Authentication Header) とIP暗号化ペイロードESP (Encapsulation Security Payload) の2つのトラフィックセキュリティプロトコル等によって実現されている。

【0029】

AHは、IPパケットの改ざんを防ぐ機能を提供し、ESPは、IPパケットを暗号化し、かつ、その認証データを格納することで、IPパケットの機密性と完全性を保証するものである。

【0030】

AH、ESP共に、認証鍵、暗号鍵を用いて、それぞれ認証情報、暗号データを作成し、送付した暗号化されたデータを解読可能な鍵を保有しているか否かにより通信相手の機器を認証する。

【0031】

図4と図5とに、それぞれ、AHプロトコルおよびESPプロトコルを利用した場合のIPパケットの構成を示す。なお、これらのパケット構成は、IPsecパケットとしてRFC2401～2403に規定されているものである。

【0032】

図4は、AHプロトコルを利用した場合のIPパケットの構成を示すものである。この場合のIPパケットは、IPヘッダ400と、TCP/UDPヘッダ402と、データ403に対するハッシュ値を格納するAHヘッダ401とを備える。

【0033】

AHヘッダ401に格納されているハッシュ値は、パケットが改ざんされていないことを証明するためのもので、通信相手間で相互に保有する認証鍵を用いて計算された値が格納される。これは、認証されているもの同士では同じ認証鍵を保有することが前提となっているもので、送信側で自身が保有する認証鍵によって計算して格納したデータのハッシュ値を、受信側が、自身が保有する認証鍵によって計算したデータのハッシュ値と比較し、両者が合致することにより、相手と同じ認証鍵を保有するものであることを確認することができる。すなわち、パケットの送信相手が同じ暗号化鍵を保有するグループ内の機器であることが証明される。

【0034】

図5はESPプロトコルを利用した場合のIPパケットの構成を示すものである。TCP/UDPヘッダと、データを暗号化した場合のヘッダ構成である。

【0035】

この場合のIPパケットは、暗号化しているパケットであることを示すESPヘッダ501と、暗号化の区切りを揃えるためのESPトレーラ504と、認証データ505とを備える。認証データ505はオプションであり、ESPヘッダ505と、暗号化されたTCP/UDPヘッダ502と、データ503と、ESPトレーラ504とのハッシュ値を格納するものである。

【0036】

認証データ505に格納されるハッシュ値は、IPペイロードの完全性を確保

し、暗号化して転送する TCP/UDP ヘッダ 502 およびデータ 503 の機密性を確保する。暗号化を行なう際には送信側が保有する暗号鍵を用いる。送信側が自身が保有する暗号鍵を用いて暗号化したデータを受信側は自身が保有する暗号鍵で復号する。受信側において、復号ができれば、相手が同じ暗号鍵を保有することが確認できる。すなわち、パケット送信相手が同じ暗号鍵を保有するグループ内機器であることの証明となる。

【0037】

また、IPsec で使用する暗号/認証アルゴリズム、鍵など、各機器間で IPsec の規格に従って通信を行う（以後、IPsec の規格に従って行う通信のことを IPsec 通信と呼ぶ）ために共有すべき情報は、セキュリティアソシエーション(SA)として管理される。

【0038】

SA は、それによって運ばれるトラフィックに対してセキュリティサービスを提供する単方向の「コネクション」である。このため、IPsec 通信を行うにあたって、通信を行う機器間で一方向の通信ごとに、予め設定を行う必要がある。すなわち、両方向の通信を行なうためには、送信方向と受信方向とのそれぞれの SA を設定する必要がある。

【0039】

なお、IPsec の詳細は、RFC 2401 "Security Architecture for the Internet Protocol" に規定されている。

【0040】

図1は、本発明を適用した一実施形態に係るグループ通信システムの構成を示す図である。

【0041】

本図に示すように、本実施形態においては、4つのノード100（100A、100B、100C、100D）がIPv6によるネットワーク110に接続されている。もちろん構成ノード数はこれに限られない。

【0042】

これらのノード100間で、ネットワーク110を介してIPパケット形式の

コマンドを送受信することにより、ノード100各々が備える機器特有のサービス機能に対する他のノード100からの操作、および、他のノード100へのサービス提供が実現される。

【0043】

具体的には、ネットワークを介して、テレビからエアコンの温度調節をしたり、テレビからの操作により、ビデオカメラで撮影している画像をビデオに送信し、ビデオカメラで撮影した画像をビデオで録画させるといったことが実現されるものである。

【0044】

例えば、ノード100A～ノード100Cは、利用者が相互にサービスを利用することを許可しているグループに属するノードであり、ノード100Dは、そのグループ外のノードとすると、グループを構成するノード100A、100B、100C間では、サービス機能の利用要求を送信する際に、要求元ノードは、グループで共有する鍵（以後、グループ鍵と呼ぶ）により計算されたハッシュ値を格納した、または、暗号化したIPパケットを送付する（101方向）。利用要求を受け取った要求先ノードは、自身の保有するグループ鍵により要求元ノードがグループ構成ノードであることを確認し、サービス機能を要求元ノードに提供する（102方向）、といったIPsec通信を行なう。

【0045】

これに対し、ノード100Dからは、サービス機能の利用要求は、通常のIPパケットによって送信することとなるため、ノード100Cに通常のIPパケットを送信すると（104方向）、ノード100Cにおいてグループ外ノードと判断され、サービス提供拒否のパケットの返答を受けることとなる（103方向）。

【0046】

ここで、ノード100Bがグループ外のノード100に提供を許可するサービスを有するノードの場合、ノード100Dからそのサービスの提供を指定して通常のIPパケットを送信すると（104b方向）、ノード100Bよりそのサービスが提供される（103b方向）。

【0047】

本実施形態では、以上のようにIPsecの仕組みを標準で実装するIPv6を用いたプロトコルによる通信が可能なネットワークを例にあげて説明する。しかし、グループを構成するノード100間に共通の暗号化鍵を持たせ、その鍵を認証鍵または暗号鍵として当該グループ間で通信を行うことができる環境を構築できるならば、通信プロトコルはこれに限られない。

【0048】

以下、このようなネットワークに接続されたノード100間で、所定のサービスの安全な利用を実現するグループの管理方法、すなわち、一つのノード100においてグループを生成し、生成されたグループに他のノード100が参加し、また、生成されたグループから離脱する方法について説明する。

【0049】

本実施形態では、空のメモ리카ードA、Bの2つを用意し、最初にグループに参加するノード100において、グループ内でIPsec通信を行うために必要な情報を生成し、そのうちの一つのメモ리카ードAに、登録する。その後参加するノード100は、メモ리카ードAから必要な情報を取得することで、グループに参加する。また、グループから離脱する際は、空のメモ리카ードBを用いる。

【0050】

図2にノード100のハードウェア構成を、図3にその機能構成を示す。

【0051】

ノード100は、ノード100が備える一つ以上の固有機能部202と、ネットワークカード205と、固有機能部202及びネットワークカード205を制御するプロセッサ200と、プロセッサ200で実行するプログラムを記憶するメモリ201と、プログラム及び設定情報を記憶するハードディスク等の外部記憶装置204と、グループ情報を受け渡すためのメモ리카ード等のインタフェースを提供する記憶媒体インタフェース206と、これらを接続するシステムバス203とを備える。

【0052】

なお、固有機能部202が実現する固有機能とは、例えばエアコンであれば、

例えば冷暖房機能、温度管理機能、タイマ機能等を司る処理部などのことである。

【0053】

また、記憶媒体インタフェース206は、挿入する記憶媒体に書き込み中であることを利用者に通知するLED（発光ダイオード）ライトを具備している。

【0054】

次に、各ノード100が備える機能を図3に従って説明する。これらの機能により、ノード100は、ネットワークを介して、利用者がサービスの相互利用を許可したグループを構成するノード100間でサービスの提供を実現する。

【0055】

各ノード100は、アプリケーション301と、グループ管理処理部302と、TCP/UDP送信処理部303と、IP送信部304と、アクセスポリシデータベース308と、SAデータベース309と、ネットワークインタフェース受信処理部310と、IP受信部314と、TCP/UDP受信処理部315と、ネットワークインタフェース送信処理部317と、記憶媒体インタフェース処理部318とを備える。

【0056】

アプリケーション301は、各ノード特有のサービスを提供するものである。

【0057】

グループ管理処理部302は、後述するグループの生成、離脱、更新など、グループに関する管理を行なうものである。

【0058】

ネットワークインタフェース受信処理部310とネットワークインタフェース送信処理部317とは、ネットワークカードを制御するものである。

【0059】

記憶媒体インタフェース処理部318は、記憶媒体インタフェース206を制御するものである。記憶媒体インタフェース318は、メモリカード等の記録媒体が記録媒体インタフェース206に挿入されたことを検出すると、記憶媒体インタフェース206に備えられているLEDライトを点灯し、メモリカードを利

用中であることを利用者に対して示す。また、グループ管理処理部 302 から処理終了の通知を受けると、記憶媒体インタフェース 206 に備えられている LED ライトを消灯し、利用者に対し、メモ리카ード等の記憶媒体への書込みが終了したこと、および、グループ管理処理部 302 における処理が完了したことを通知する。

【0060】

なお、通知を受けた利用者は、メモ리카ードを当該記憶媒体インタフェース 206 から取り出すことができる。

【0061】

TCP/UDP 送信処理部 303 と、IP 送信部 304 と、IP 受信部 314 と、TCP/UDP 受信処理部 315 とは、送受する IP パケットに対し、各層の処理を行い、通信を実現するものである。

【0062】

IP 送信部 304 は、IPv6 送信前処理部 305 と、IPsec 送信処理部 306 と、IPv6 後処理部 307 とを備え、IP 受信部 314 は、IPv6 受信前処理部 311 と、IPsec 受信処理部 312 と、IPv6 受信後処理部 313 とを備える。IP 送信部 304 と IP 受信部 314 とで、IPv6 による通信を実現する。

【0063】

ここで、IPv6 受信前処理部 311 は、IP ヘッダを構成するバージョン、ペイロード長、ホップ・リミットの設定値の確認およびオプションヘッダ（AH と ESP とを除く）処理といった IPv6 受信前処理を行なうものである。IPv6 受信前処理部 311 は、受け取った IP パケットに AH ヘッダまたは ESP ヘッダのいずれかが付加されていた場合、その IP パケットを IPsec 処理部 312 に受け渡す。いずれのヘッダも付加されていなかった場合、その IP パケットを後述する受信アクセス制御部 316 に受け渡す。

【0064】

IPsec 処理部 312 は、IP ヘッダのオプションヘッダのうち、AH と ESP の処理を行ない、受信した IP パケットがグループに属するノード 100 か

ら送信されたものか否かを判断する。

【0065】

IPv6 受信後処理部 313 は、IP パケットを受け取ると、送信元 IP アドレス、送信先 IP アドレスを含む Pseudo Header を作成し、受け取った IP パケットの IP ヘッダと置き換え、TCP/UDP 受信処理部 315 に受け渡すといった IPv6 受信後処理を行なう。

また、IP 受信部 314 は、受信アクセス制御部 316 をさらに備える。

【0066】

受信アクセス制御部 316 は、IPv6 受信前処理部 311 から、AH ヘッダまたは ESP ヘッダを有していない IP パケットを受け取り、当該 IP パケットのアプリケーションへのアクセスを制御するものである。

【0067】

SA データベース 309 は、IPsec で必要なセキュリティアソシエーション (SA) が格納されているものである。

【0068】

アクセスポリシデータベース 308 は、グループ内での通信を実現するため、各ノードに対するアクセス制御に関する情報及びグループ情報が格納されているものである。

【0069】

アクセスポリシデータベース 308 は、グループ管理テーブル 600 と、アクセス制御対象アプリケーション管理テーブル 700 と、グループメンバ管理テーブル 800 とを備える。

【0070】

なお、グループ管理テーブル 600 は、記憶媒体インタフェース 206 を介してノードに接続される記憶媒体であるメモリカード上でも保持されるものである。

【0071】

以下、グループ管理処理部 302、アクセスポリシデータベース 306 の各データベース、および、SA データベース 309 内の SA について、その詳細を説

明する。

【0072】

図6に、グループ管理処理部302の機能構成図を示す。

【0073】

本図に示すように、グループ管理処理部302は、制御部3100と、グループ生成処理部3200と、グループ参加処理部3300と、グループ離脱処理部3400と、グループ情報更新処理部3500と、グループ制御IPパケット受信処理部3600とを備える。

【0074】

グループ管理処理部302は、ユーザがメモリカードを記憶媒体インタフェース206に挿入したことを検出した記憶媒体インタフェース処理部318からの指示で処理を開始する。

【0075】

制御部3100は、記憶媒体インタフェース処理部318からの指示を受け、挿入されたメモリカード内と、自身が保有するアクセスポリシデータベース308を検索し、グループ管理テーブル600の有無を確認する。

【0076】

グループ生成処理部3200は、グループ自体が存在しない場合に、新たにグループを生成するグループ生成処理を行なう。グループ生成処理は、制御部3100がメモリカードにもアクセスポリシデータベース308にもグループ管理テーブル600が存在しないと判断した場合に行なわれるものである。

【0077】

具体的には、グループに属する他のノードと暗号通信を行なうために必要な情報、すなわち、グループ管理テーブル600に登録すべき項目を生成、選択し、グループ管理テーブル600を作成し、それを、メモリカードおよびアクセスポリシデータベース308に登録する。

【0078】

グループ参加処理部3300は、既存のグループに、新たなメンバとして自身を参加させるグループ参加処理を行なうものである。グループ参加処理は、制御

部 3100 がメモリカードにはグループ管理テーブル 600 が存在するが、アクセスポリシデータベース 308 にグループ管理テーブル 600 が存在しないと判断した際に行われるものである。

【0079】

グループ参加処理部 3300 は、挿入されたメモリカードに格納されている暗号通信に必要な情報を取得し、また、自身のノード 100 と暗号通信を行なうために必要な情報をグループに既に属している他のノード 100 に送信する。具体的には、メモリカード内のグループ管理テーブル 600 に自身の情報を追加し、自身の情報が追加されたグループ管理テーブル 600 を、アクセスポリシデータベース 308 に登録する。

【0080】

また、グループ管理テーブル 600 から得た、グループに既に属しているノード 100 のホスト名から IP アドレスを解決することで、グループメンバ管理テーブル 800 を生成する。

【0081】

さらに、グループ参加処理部 3300 は、グループ内の各ノード 100 と IPsec 通信が可能となるように、セキュリティアソシエーションの設定を行ない、SA データベース 309 に登録し、グループ内の既存のメンバのノード 100 に、IPsec 通信で自身が追加されたことを通知する。

【0082】

グループ離脱処理部 3400 は、グループから離脱するグループ離脱処理を行なうものである。

【0083】

本実施形態では、ユーザが所定のノード 100 をグループから離脱させたい場合、当該ノード 100 に空のメモリカードを挿入することとする。すなわち、グループ離脱処理は、制御部 3100 が、自身のアクセスポリシデータベース 308 にはグループ管理テーブル 600 が存在するが、挿入されたメモリカードにはグループ管理テーブル 600 が存在しないと判断した際に行われるものである。

【0084】

グループ離脱処理は、グループに属する他のノード100に自身のノード100が離脱することを通知し、当該グループ内で暗号通信を行なうために必要な情報、すなわち、自身のアクセスポリシデータベース308およびSAデータベース309内のグループ間の通信に係わるデータを削除するものである。

【0085】

ここで、グループ参加処理部3300およびグループ離脱処理部3400がそれぞれ、参加および離脱をグループに属する各ノード100に通知する際は、グループ制御IPパケットと呼ぶ特別なデータ部を有するIPパケットを用いる。

【0086】

ここで、そのグループ制御IPパケットについて説明する。図7にグループ制御IPパケットのデータ部1000の一例を示す。

【0087】

本図に示すように、グループ制御IPパケットのデータ部1000は、コマンド識別子を格納するコマンド識別子格納部1001と、IPアドレスとホスト名とをそれぞれ格納する、16バイトのIPアドレス格納部1002と、ホスト名格納部1003とを備える。

【0088】

ここで、新規参加を通知する際にグループに属する各ノード100に送信されるグループ制御IPパケットの場合、コマンド識別子格納部1001に「加入」を示す(00) hexが設定される(以後、本グループ制御IPパケットを加入コマンドと呼ぶ)。そして、IPアドレス格納部1002と、ホスト名格納部1003とには、それぞれ自身のアドレスとホスト名とが設定される。

【0089】

また、グループから離脱する際にグループに属する各ノード100に送信されるグループ制御IPパケットの場合、コマンド識別子格納部1001に「離脱」を示す(01) hexが設定される(以後、本グループ制御IPパケットを離脱コマンドと呼ぶ)。そして、IPアドレス格納部1002と、ホスト名格納部1003とには、それぞれ自身のアドレスとホスト名とが設定される。

【0090】

グループ情報更新処理部 3 5 0 0 は、グループ管理テーブル 6 0 0 の内容を更新したり、それをメモ리카ードにコピーするといったグループ情報更新処理を行なうものである。

【 0 0 9 1 】

本実施形態においては、セキュリティを向上させるために、グループ内で利用するグループ鍵が所定の期間ごとに更新される設定となっている。グループ情報更新処理部 3 5 0 0 は、グループ管理テーブル 6 0 0 の鍵有効期限がタイムアウトした時点で、新しいグループ鍵を生成する。

【 0 0 9 2 】

ここで、グループ管理テーブル 6 0 0 生成時に、ノード毎に、異なる鍵有効期限が設定される。具体的には、所定の有効期限の、例えば、プラスマイナス 3 0 % 間のランダムな値を、その鍵有効期限に加算あるいは減算することで得られた値を鍵有効期限として各ノードに設定する。このため、各ノードで鍵有効期限のタイムアウトが異なるタイミングで生じ、鍵の更新を行なうノードが一つに定まり、グループのメンバが同時にグループ鍵を生成することを避けることができる。

【 0 0 9 3 】

そして、更新されたグループ鍵を更新前のグループ鍵で暗号化し、グループ鍵を更新したメンバからグループに属する各ノードに送付する。このとき、鍵の更新とともに、各ノードの鍵有効期限を再設定してもよい。

【 0 0 9 4 】

また、グループ情報更新処理部 3 5 0 0 は、他のノードから、更新されたグループ鍵を受信した場合、自身の保有するグループ鍵の情報を更新するとともに、グループに属する各ノード 1 0 0 の I P アドレスが更新された場合、関連するデータベース内の I P アドレスを更新する。

【 0 0 9 5 】

ここで、本実施形態では、グループの鍵の更新は上述のように行なわれるため、グループ参加処理に用いられるメモ리카ード内のグループ管理テーブル 6 0 0 には反映されない。同様に、上述のグループからの離脱処理は、空のメモ리카ー

ドを用いて行なわれ、離脱したノード 1 0 0 からグループを構成する他のノード 1 0 0 への通知は、I P s e c 通信によって行われる。このため、グループ離脱によるグループ構成メンバの変更も、グループ参加処理に用いられるメモリカード内のグループ管理テーブル 6 0 0 に反映されない。

【0 0 9 6】

このため、本実施形態では、グループ情報更新処理部 3 5 0 0 が、メモリカード内のグループ管理テーブル 6 0 0 の更新処理も行なう。

【0 0 9 7】

グループ情報更新処理部 3 5 0 0 が行なうメモリカード内のグループ管理テーブル 6 0 0 の更新処理は、制御部 3 1 0 0 が、自身のアクセスポリシデータベース 3 0 8 にも、挿入されたメモリカードにもグループ管理テーブル 6 0 0 が存在すると判断した際に行われるものである。

【0 0 9 8】

グループ情報更新処理部 3 5 0 0 は、当該ノード 1 0 0 のアクセスポリシデータベース 3 0 8 に格納されているグループ管理テーブル 6 0 0 の情報をメモリカード内のグループ管理テーブル 6 0 0 にコピーする。

【0 0 9 9】

本実施形態では、実際のグループ参加処理において、グループ参加処理を行なう場合に、グループに既に所属しているノード 1 0 0 にメモリカードを挿入し、メモリカード内のグループ管理テーブル 6 0 0 を最新のものとする処理を前もって行なうよう手順を定めておく。

【0 1 0 0】

グループ制御 I P パケット受信処理部 3 6 0 0 は、前述のグループ制御 I P パケットを受信した際の処理を行うものである。

【0 1 0 1】

具体的には、加入コマンドを受信した場合は、I P アドレス格納部 1 0 0 2 およびホスト名格納部 1 0 0 3 に格納されている I P アドレスおよびホスト名を自身のグループ管理テーブル 6 0 0 およびグループメンバ管理テーブル 8 0 0 とに追加し、送信元ノード 1 0 0 と暗号通信を行なうために必要なセキュリティアソ

シエーションを作成する。一方、離脱コマンドを受信した場合は、それらを削除する。

【0102】

次に、アクセスポリシデータベース308に格納されるグループ管理テーブル600とアクセス制御対応アプリケーション管理テーブル700と、グループメンバ管理テーブル800とについて以下に説明する。

【0103】

グループ管理テーブル600は、グループに属するノード100を識別するための情報とグループで共有する鍵の情報とを格納するテーブルである。図8にその一例を示す。

【0104】

本図に示すようにグループ管理テーブル600は、ネットワークに接続されたノード100によって構成されるグループを識別するためのグループ識別子を格納するグループ識別子格納フィールド601と、グループ鍵を格納するグループ鍵格納フィールド602と、そのグループ鍵の有効期限を格納するグループ鍵有効期限格納フィールド603と、AH、ESPといったグループ内で通信に利用するIPsecの機能の種別を格納するIPsec種別格納フィールド604と、認証あるいは暗号に用いるアルゴリズムを格納するアルゴリズム格納フィールド605と、グループに属するノード100を識別する情報であるホスト名を格納するホスト名格納フィールド606（606A～606B）とを備える。

【0105】

アクセス制御対象アプリケーション管理テーブル700は、ノード100にグループ外のノード100が利用可能なアプリケーションが実装されている場合、ノード100に実装されている各アプリケーションに対するアクセス制御のために用いる情報が格納されているテーブルである。

【0106】

なお、本テーブルは、ノード100がグループ内からのアクセスに対してのみ提供するアプリケーションだけを実装している場合は不要なものである。

【0107】

アクセス制御対象アプリケーション管理テーブル 700 の一例を図 9 に示す。

【0108】

本図に示すように、アクセス制御対象アプリケーション管理テーブル 700 は、グループ外のノード 100 にも開放されているアプリケーションが利用するポート番号を格納するポート番号格納フィールド 701 (701A、701B) を備える。各ノード 100 は、IP パケット受信時に、本テーブルを参照し、当該 IP パケットがアクセスしようとしているアプリケーションがグループ外のノード 100 にも開放されたアプリケーションであるか否かの判定を行う。

【0109】

次に、グループメンバ管理テーブル 800 について説明する。各ノード 100 間で、IPv6 に基づき、IP パケット通信を行なうためには、各ノード 100 の IP アドレスを知る必要がある。グループに属する各ノード 100 の IP アドレスは、グループ参加時に取得した各ノード 100 のホスト名から ICMP (Internet Control Message Protocol) Echo Request/Reply パケットのやりとりにより、アドレスの解決を行なうことで取得する。このように、グループメンバ管理テーブル 800 は、各ノードにおいてホスト名から IP アドレスを解決して作成するもので、そこには、グループに属する各ノード 100 のホスト名と IP アドレスとの対応が格納されている。

【0110】

図 10 にグループメンバ管理テーブル 800 の一例を示す。

【0111】

本図に示すように、本テーブルは、ノードを特定するホスト名を格納するホスト名格納フィールド 801 と、ホスト名と対応させて各ノード 100 の IP アドレスを格納する IP アドレス格納フィールド 802 と、IP アドレスの有効期限を格納する有効期限格納フィールド 802 とを備える。

【0112】

ノード 100 が再起動した場合などに、ノード 100 の IP アドレスは変わる可能性がある。また、一定時間内に IP アドレス格納部 802 に格納されている IP アドレスと送受信が行われないと、有効期限が切れる場合がある。

【0113】

このようなノードに対しIPパケットを送信する場合、ノード100のIPv6送信前処理部305は、ICMP Echo Request/Replyパケットのやりとりにより、ホスト名からアドレスの解決を再度行ない、グループ管理処理部302に通知する。それを受けて、グループ管理処理部302のグループ情報更新処理部3500は、IPアドレスが登録されている本テーブルおよびグループ内の通信に利用するセキュリティアソシエーションを更新する。

【0114】

次に、SAデータベース309に格納されている、セキュリティアソシエーション900について説明する。セキュリティアソシエーション900は、IPsecにのっとり通信を行うために共有すべき情報を管理するものであり、例えば、ノード100Aとノード100B間で通信する場合、ノード100Aからノード100B方向の通信、および、ノード100Bからノード100A方向の通信、両者に対し、独立して設定する必要があるものである。

【0115】

図11に、セキュリティアソシエーション900の一例を示す。

【0116】

本図に示すように、セキュリティアソシエーション900は、各セキュリティアソシエーションを識別するSPI(セキュリティポリシ識別子)、送信元IPアドレス、送信先アドレス、プロトコルとして認証あるいは暗号の指定、暗号範囲としてトランスポートモードあるいはトンネルモードの指定、暗号アルゴリズム、暗号鍵、認証アルゴリズム、認証鍵、鍵の有効期限などを含む。

【0117】

本実施形態では、各ノード100においてセキュリティアソシエーション900を作成するにあたり、送信用のセキュリティアソシエーション900を作成する場合は、送信元IPアドレスには、自身のノード100のIPアドレスを、送信先IPアドレスには、通信相手先ノードのIPアドレスを設定し、受信用を作成する場合は、送信元IPアドレスには、通信相手先のIPアドレスを設定し、送信先IPアドレスには、自身のノード100のIPアドレスを設定する。

【0118】

SPIには、送信用、受信用ともに、グループ管理テーブル600のグループ識別子格納部601に格納されているグループ識別子が格納される。また、送信用、受信用ともに、プロトコル、認証鍵アルゴリズム、認証鍵、有効期限には、それぞれ、グループ管理テーブル600に格納されているものが設定される。

【0119】

以上、本実施形態におけるノード100の各機能などについて説明した。

【0120】

次に、本実施形態における、ネットワーク110に接続された各ノード100間で、グループを生成し、参加する手順、また、一旦参加したグループから離脱する手順などを説明する。

【0121】

以下においては、IPsecの機能種別としてAHを、モードとしてトランスポートモードを、認証アルゴリズムとしてSHA-1 (Secure Hash Algorithm 1:SHS(Secure Hash Standard) FIPS 180として規定) を用いる場合を例にあげ、説明する。IPsec通信の設定は、これらに限られない。

【0122】

また、本実施形態においては、前述したように、グループの情報を格納するメモリカードと、グループを離脱する際に用いる空のメモリカードとの2つのメモリカードを用いてグループの生成、参加、離脱、情報更新などを行なう。

【0123】

図12に、グループ管理処理部302が行なうグループ管理処理手順3020を示す。

【0124】

グループ管理処理手順3020は、ユーザがメモリカードを各ノード100の記録媒体インタフェース206に挿入することをきっかけに開始される。

【0125】

そして、ノード100の記憶媒体インタフェース処理部318は、メモリカードが記録媒体インタフェース206に挿入されたことを検出すると、記憶媒体イ

インタフェース 206 に備えられている LED ライトを点灯し、メモリカードを利用中であることを利用者に対して示す。

【0126】

LED ライトが消灯されたことにより、ユーザは処理が終了したことを知り、メモリカードを取り出すことができる。

【0127】

また、記憶媒体インタフェース処理部 318 は、メモリカードを検出したことをグループ管理処理部 302 へ通知する。その通知を受けて、グループ管理処理部 302 は、グループ管理処理 1000 を開始する。

【0128】

まず、グループ管理処理部 302 の制御部 3100 は、自身のアクセスポリシデータベース 308 と、記録媒体インタフェース処理部 318 を介してメモリカード挿入されたメモリカードとにアクセスし、グループ管理テーブル 600 の有無を確認する（ステップ 3021）。

【0129】

ここで、どちらにもグループ管理テーブル 600 がない場合、グループ自体が存在しない、すなわち、グループを生成する必要があると判断し、制御部 3100 は、グループ生成処理部 3200 にグループ生成処理 3210 を行わせる（ステップ 3022）。グループ生成処理 3210 が完了すると、制御部 302 は、記憶媒体インタフェース処理部 318 に対し、メモリカードの書き込み終了を通知し（ステップ 3027）、処理を終える。

自身のアクセスポリシデータベース 302 には無く、メモリカードには存在した場合、制御部 3100 は、メモリカードに存在するグループに自身が参加しようとしていると判断し、グループ参加処理部 3300 にグループ参加処理 3310 を行なわせ（ステップ 3023）、グループ参加処理が完了すると、ステップ 3027 に進む。

【0130】

メモリカードには無く、自身のアクセスポリシデータベース 302 には存在した場合、制御部 3100 は、自身は既にグループに属しているが空白のメモリカ

ードが挿入されたことにより、グループ離脱処理を行なうものと判断し、グループ離脱処理部 3400 にグループ離脱処理 3410 を行なわせ（ステップ 3026）、グループ離脱処理が完了するとステップ 3027 に進む。

【0131】

どちらにもグループ管理テーブル 600 が存在する場合は、制御部 3100 は、まず、アクセスポリシデータベース 302 内のグループ管理テーブル 600 とメモ리카ード内のグループ管理テーブル 600 とのグループ識別子を比較する（ステップ 3024）。

【0132】

ここで、両者が同じであれば、メモ리카ードのグループ情報を更新する処理を行なうものと判断し、グループ情報更新処理部 3500 にグループ情報更新処理 3510 としてアクセスポリシデータベース 302 内のグループ管理テーブル 600 をメモ리카ードにコピーする処理を行なわせ（ステップ 3025）、当該処理が完了すると、ステップ 3027 に進む。

【0133】

ステップ 3024 において、両者が異なった場合、制御部 3100 は、誤ったメモ리카ードが挿入されたと判断し、そのままステップ 3027 にすすむ。

【0134】

次に、グループ生成処理 1200、グループ参加処理 1300、グループ離脱処理 1600、グループ情報更新処理 1500 の手順を説明する。

【0135】

まず、グループ生成処理 3210 の処理手順を図 13 に示す。

【0136】

制御部 3100 から処理開始の指示を受けると、グループ生成処理部 3200 は、グループ鍵を生成し（ステップ 3211）、グループを識別するためのグループ識別子を生成し（ステップ 3212）、認証・暗号モードとして認証（AH）を選択し（ステップ 3213）、アルゴリズムとして SHA-1 を選択する（ステップ 3214）。

【0137】

そして、それぞれを、グループ鍵格納フィールド 6 0 2、グループ識別子格納フィールド 6 0 1、I P s e c 種別格納フィールド 6 0 4、アルゴリズム格納フィールド 6 0 5 に格納し、グループ管理テーブル 6 0 0 を作成する（ステップ 3 2 1 5）。そして、ホスト名格納フィールド 6 0 6 に自ノード 1 0 0 のホスト名を登録する（ステップ 3 2 1 6）。

【0 1 3 8】

グループ管理テーブル 6 0 0 が完成すると、グループ生成処理部 3 2 0 0 は、本テーブルをメモリカードにコピーすると共に、自ノード 1 0 0 のアクセスポリシデータベース 3 0 8 に記憶し（ステップ 3 2 1 7, 3 2 1 8）、処理が終了したことを制御部 3 1 0 0 に通知する。

【0 1 3 9】

次に、グループ参加処理 3 3 1 0 の処理手順を図 1 4 に示す。

【0 1 4 0】

制御部 3 1 0 0 から処理開始の指示を受けると、グループ参加処理部 3 3 0 0 は、メモリカード上のグループ管理テーブル 6 0 0 のホスト名格納フィールド 6 0 6 に自ノード 1 0 0 のホスト名を追加し（ステップ 3 3 1 1）、メモリカード上のグループ管理テーブル 6 0 0 を自身のアクセスポリシデータベース 3 0 8 内に記憶する（ステップ 3 3 1 2）。

【0 1 4 1】

次に、グループメンバ管理テーブル 8 0 0 を作成するとともに、グループに既に属している各ノード 1 0 0 に、自身の参加を通知する新メンバ通知処理 3 7 1 0 を行なう（ステップ 3 3 1 3）。

【0 1 4 2】

そして、今までのステップで記録されたグループ管理テーブル 6 0 0 の情報およびグループメンバ管理テーブル 8 0 0 の情報とを用い、各ノード 1 0 0 との I P s e c 通信に用いるセキュリティアソシエーション 9 0 0 を生成し（ステップ 3 3 1 4）、処理が終了したことを制御部 3 1 0 0 に通知する。

【0 1 4 3】

ここで、新メンバ通知処理 3 7 1 0 についてその処理手順を説明する。図 1 5

にその処理手順を示す。

【0 1 4 4】

新メンバ通知処理 3 7 1 0 では、グループ管理テーブル 6 0 0 内のホスト名フィールド 6 0 6 に格納されているホストごとに順に、I C M P Echo Request / Replyにより I P アドレスを取得し（ステップ 3 7 1 2）、グループメンバ管理テーブル 8 0 0 に、ホスト名ごとに取得した I P アドレスを登録する（ステップ 3 7 1 3）。

【0 1 4 5】

上記のステップで取得した、グループを構成する各ノード 1 0 0 の I P アドレスに対して加入コマンドを生成し（ステップ 3 7 1 4）、それを送信する（ステップ 3 7 1 5）。

【0 1 4 6】

そして、次のホスト名を読み出して、ステップ 1 3 3 0 から 1 3 6 0 の処理を繰り返す（ステップ 3 3 1 6）。ここで、読み出したホスト名が自身のホスト名の場合は、何も処理を行わず、次のホスト名を読み出す（ステップ 3 7 1 1）。そして、グループ管理テーブル 6 0 0 のホスト名格納フィールド 6 0 6 に格納されている、自身のノード 1 0 0 を除く全てのノードに対して以上の処理を終えると（ステップ 3 7 1 7）、グループ内への新メンバ通知処理 1 3 3 0 を終える。

【0 1 4 7】

以上、グループ参加処理 3 3 1 0 について説明した。

【0 1 4 8】

次に、グループ離脱処理 3 4 1 0 について、図 1 6 を用いて説明する。

【0 1 4 9】

制御部 3 1 0 0 から処理開始の指示を受けると、グループ離脱処理部 3 4 0 0 は、ノード 1 0 0 内のグループ管理テーブル 6 0 0 のホスト名格納部 6 0 6 に登録されているホスト名を順番に読み出す（ステップ 3 3 1 1）。

【0 1 5 0】

ここで、読み出したホスト名が自ホスト名と一致した場合は、次のホスト名を読み出す。

【0151】

読み出したホスト名が自ホスト名と一致しない場合は、グループメンバ管理テーブル800から読み出したホスト名に対応するIPアドレスを検索する（ステップ3312）。以後、このIPアドレスを検索したIPアドレスと呼ぶ。

【0152】

次に、送信先IPアドレスを検索したIPアドレスとした離脱コマンドを作成し（ステップ3313）、その送信先IPアドレスを有するノード100に送信する（ステップ3314）。

【0153】

グループ離脱処理部3400は、自身の保有するグループメンバ管理テーブル800から以上の操作を行なった検索したIPアドレスに係わるデータを削除する（ステップ3315）。

【0154】

次に、SAデータベース309に記憶されているセキュリティアソシエーション900から検索したIPアドレスと等しい送信先IPアドレスを持つものを抽出し、そのセキュリティアソシエーション900を削除する（ステップ3316）。

【0155】

また、検索したIPアドレスと等しい送信元IPアドレスを持つセキュリティアソシエーション900を抽出し、それを削除する（ステップ3317）。

【0156】

グループ離脱処理部3400は、グループ管理テーブル600に登録されている全てのホスト名に対して、以上のステップ3311～ステップ3317の処理を実行した後（ステップ3318）、自身が保有するグループ管理テーブル600を削除し（ステップ3319）、グループ離脱処理3310を終了する。そして、制御部3100に処理終了を通知する。

【0157】

次に、上記のグループ参加処理3310内のグループ内への新メンバ通知処理3710のステップ3715およびグループ離脱処理3310のステップ331

4において送信された、それぞれ加入コマンドおよび離脱コマンドを受信した場合の各ノード100側での処理を以下に説明する。

【0158】

本処理は、グループ制御IPパケット受信処理部3600によって行なわれ、グループ制御IPパケット受信処理3610と呼ぶ。図17に本処理の手順を示す。

【0159】

グループを構成する各ノード100は、ネットワークインタフェース受信処理部310においてグループ制御IPパケットを受信すると、IP受信部314、TCP/UDP受信処理部315を経てグループ管理処理部302のグループ制御IPパケット受信処理部3600へ受け渡す。

【0160】

受信したグループ制御IPパケット受信処理部3600は、コマンド識別子格納部1001に設定されているコマンド識別子が加入であるか否かを確認する（ステップ3611）。

【0161】

ステップ3611でコマンド識別子が加入を示す(00) hexであった場合、すなわち、加入コマンドを受信した場合、ステップ3612に進み、グループ制御IPパケットのホスト名1003に設定されている加入コマンドを送信してきたノード100のホスト名をグループ管理テーブル600に登録する（ステップ3612）。

【0162】

そして、グループメンバ管理テーブル800に、加入コマンドを送信してきたノード100のホスト名と、グループ制御IPパケットのIPアドレス格納部1002に設定されているそのIPアドレスとを登録する（ステップ3613）。

【0163】

次に、グループ制御IPパケット受信処理部3600は、送信用、すなわち、自身のノード100から加入コマンドを送信してきた新規に加入したノード100方向の送信、および、受信用、すなわち、加入コマンドを送信してきた新規に

加入したノード100から自身のノード100方向の送信、各々のセキュリティアソシエーション900を作成する処理を行なう（ステップ3614、3615）。

【0164】

次に、ステップ3611でコマンド識別子が離脱を示す(01) hexであった場合、すなわち、離脱コマンドを受信した場合、グループ制御IPパケット受信処理部3600は、ステップ3616に進む。

【0165】

ここで、グループ制御IPパケット受信処理部3600は、SAデータベース309に記憶されているセキュリティアソシエーション900から、受信したグループ離脱コマンドのデータ部1000のIPアドレス1002に格納されているIPアドレスと等しい送信先IPアドレスを持つものを抽出し、抽出したセキュリティアソシエーションを削除する（ステップ3616）。

【0166】

次に、受信した離脱コマンドのIPアドレス1002と等しいIPアドレスを有するデータをグループメンバ管理テーブル800から削除し（ステップ3617）、受信した離脱コマンドのホスト名1003に格納されているホスト名と等しいホスト名を、自ノード100上のグループ管理テーブル600から削除する（ステップ3618）。

【0167】

グループ内の全てのノード100において以上の手順を行なうことにより、全てのノード100が保有する離脱したノード100に対応するセキュリティアソシエーション900を削除し、また、グループ管理テーブル600から、離脱したノード100の情報を削除する。

【0168】

以上のようにして、グループを構成するノード100に新規加入または離脱といった変更があった場合、当該ノード100から送信されるグループ制御IPパケットを受信した他のノード100において、自身の保有するセキュリティアソシエーションおよびグループ管理テーブル600が更新される。

【0 1 6 9】

以上、グループ制御 I P パケット受信処理を説明した。

【0 1 7 0】

ここまで、グループ管理処理部 3 0 2 による、グループの生成、参加、離脱などのグループ管理処理について説明した。

【0 1 7 1】

次に、上記の手順で生成され管理されているグループ内で、アプリケーションを互いに利用する手順を以下に説明する。

【0 1 7 2】

アプリケーションの利用は、I P パケットを互いに送受することによって行なわれる。まず、この I P パケットの送受信について説明する。

【0 1 7 3】

前述のように、I P s e c 通信を行うために予め設定の必要なセキュリティアソシエーション 9 0 0 は、グループ管理処理 3 0 2 において、新たなグループ構成メンバが追加される際に生成される。すなわち、グループに属している限り、I P s e c 通信は可能である。

【0 1 7 4】

I P パケットを送信するにあたり、I P s e c 送信処理部 3 0 6 は、送信する I P ヘッダの送信先 I P アドレスをキーに、S A データベース 3 0 9 を検索し、対応する I P アドレスが送信先 I P アドレスとして格納されているセキュリティアソシエーション 9 0 0 を抽出する。抽出したセキュリティアソシエーション 9 0 0 に登録されている情報に基づき、I P s e c 処理を行い、I P v 6 送信後処理 3 0 7 を行い、ネットワークインタフェース送信処理部を介して、送信先ノードに I P パケットを送信する。

【0 1 7 5】

次に、I P パケット受信時の処理手順を図 1 8 を用いて説明する。

【0 1 7 6】

ネットワークインタフェース受信処理部 3 1 0 を介して I P パケットを受信すると、I P v 6 受信前処理部 3 1 1 は、I P v 6 受信前処理を行い（ステップ 4

010)、受信したIPヘッダ内の、AHヘッダの有無をチェックする(ステップ4020)。

【0177】

受信したIPヘッダ内にAHヘッダ401があると判断したならば、そのIPパケットをIPsec受信処理部312に受け渡す。

【0178】

受け取ったIPsec受信処理部312は、後述するIPsec受信処理3120を行い(ステップ4030)、IPv6受信後処理部313にIPパケットを受け渡す。

【0179】

そして、IPv6受信後処理部313は、IPv6受信後処理3130を行い(ステップ4040)、処理を終了する。

【0180】

なお、ここで、IPv6受信後処理部313は、IPv6受信後処理3130を終えた受信したパケットをTCP/UDP受信処理部315に受け渡す。受け取ったTCP/UDP受信処理部315は、受け取ったパケットの受信処理を行い、アプリケーション301に受信データとして渡す。

【0181】

ステップ4020で、上記のヘッダがないと判断した場合、そのIPパケットを受信アクセス制御部316に受け渡す。

【0182】

受け取った受信アクセス制御部316は、それがICMPパケットであるか否かチェックする(ステップ4050)。

【0183】

ステップ4050で、受信したIPパケットが、ICMPパケットであると判断されたならば、そのままIPv6受信後処理部313に受け渡し、IPv6受信後処理3130を行い(ステップ4040)、処理を終了する。

【0184】

ステップ4050で、ICMPパケットではないと判断されたならば、受信ア

アクセス制御部 316 は、その IP パケットをグループ外のノード 100 から送信されたグループ外 IP パケットであると判断し、後述するグループ外 IP パケット受信処理 3160 を行い（ステップ 4060）、処理を終了する。

【0185】

次に、上記の IPsec 処理 3120 について説明する。

【0186】

IPsec 処理部 312 は、AH ヘッダを有する IP パケットを受信すると、IP ヘッダの送信元 IP アドレス、送信先 IP アドレス、AH ヘッダ 401 に設定されている SPI が一致するセキュリティアソシエーション 900 を SA データベース 309 から抽出する。

【0187】

そして、抽出したセキュリティアソシエーション 900 に記憶されている認証鍵を用いて受信した IP パケットの認証情報を作成し、AH ヘッダ 401 に設定されている認証情報と比較する。

【0188】

両者が一致していれば、受信した IP パケットをグループに属する正当なノード 100 からの送信とみなし、IPv6 受信後処理部 313 に受け渡す。そして、一致しない場合は、その IP パケット破棄する。

【0189】

以上 IPsec 処理 3120 について説明した。

【0190】

次に、受信アクセス制御部 316 によるグループ外パケット受信処理 3160 について説明する。

【0191】

以上のように、本実施形態においては、グループに属するノード 100 は、グループ外のノード 100 から、AH ヘッダを有する IP パケットを受信した場合は、IPsec 通信処理部 312 において、また、AH ヘッダを有しない IP パケットを受信した場合は、IPv6 受信前処理部 311 において、当該 IP パケットが、IPv6 受信後処理部 313、TCP/UDP 受信処理部 315 を介し

てアプリケーション 301 に到達することを排除している。

【0192】

しかし、本実施形態においては、ノード 100 によっては、その保有するアプリケーションの利用を、グループ外のノード 100 にも開放しているものがある。前述したように、このようなアプリケーションを有するノード 100 は、アプリケーションごとのポート番号を、アクセス制御対象アプリケーション管理テーブル 700 において管理している。

【0193】

グループ外のノード 100 から AH ヘッダを有する IP パケットを受信した場合は、その IP パケットを復号することができないため、それは IPsec 通信処理部 312 において破棄することは先に説明した。

【0194】

グループ外 IP パケット受信処理 3160 は、グループ外のノード 100 から通常の IP パケットを受信した際に、グループ外のノード 100 に開放しているアプリケーションに当該 IP パケットを送達する処理である。

【0195】

グループ外 IP パケット受信処理 3160 では、IP パケットを受け取ったノード 100 が、グループ外のノード 100 に対し何らサービス機能を提供しない場合、アクセスエラーをデータとして格納した IP パケットを送信元に対して送信し、受信した IP パケットは破棄する。これに対し、グループ外のノード 100 に対して何らかのサービス機能を提供する場合は、アクセス制御対象アプリケーション管理テーブル 700 の登録に従って、アプリケーションを提供するよう制御している。

【0196】

以下にその手順を図 19 を用いて説明する。

【0197】

受信アクセス制御部 316 は、IPv6 受信前処理部 311 から ICMP パケットではない IP パケットを受信した場合、当該 IP パケットから読取った送信先ポート番号とアクセス制御対象アプリケーション管理テーブル 700 に登録さ

れているポート番号701との比較を行なう（ステップ3161）。

【0198】

アクセス制御対象アプリケーション管理テーブル700には、グループ外のノードに利用が許可されているアプリケーションのポート番号が登録されているため、両者が一致した場合、サービス機能を要求元ノード100に提供できることとなる。

【0199】

この場合、受信アクセス制御部316は、受け取ったIPパケットをIPv6受信後処理部313に受け渡し、受け取ったIPv6受信後処理部313は、IPv6受信後処理3130を行なう（ステップ3164）。

【0200】

そして、IPv6受信後処理部313から処理されたIPパケットを受け取ったTCP/UDP受信処理部315は、それを、アプリケーション301に受け渡す。

【0201】

ステップ3161において、ポート番号が一致しない場合は、提供できるサービス機能がないため、受信アクセス制御部316は、アクセスエラーをデータとして格納したIPパケットを生成しIP送信部304から送信元に送信し（ステップ3162）、受信したIPパケットは破棄する（ステップ3163）。

【0202】

以上、グループ外IPパケット受信処理について説明した。

【0203】

このように、本実施形態においては、グループ内のノード100間ではIPsec通信を行い、グループ外のノード100とは通常のIPパケットによる通信を行うことで、アクセス制御対象アプリケーション管理テーブル700で管理している各アプリケーションのポート番号に従って、アプリケーションごとにグループ内外のアクセス許可を制御することができる。これにより、一つのノード100において、グループだけで利用するサービス機能と、誰もが利用できるサービス機能とを実装し、それぞれへのアクセス制御を可能としている。

【0204】

本実施形態によれば、ホームネットワークを構成するノード100において作成したグループ鍵を含むIPsec通信に必要な情報を、共通のメモリカードを介して、利用者が相互に利用することを許可する各ノード100に配布する。

【0205】

配布されたノード100は、グループに所属している他のノード100とIPsec通信ができるように、セキュリティアソシエーション900を設定するとともに、新規加入したことを、グループに所属している他のノード100に通知する。

【0206】

通知を受けたノード100は、それぞれ、新規に加入したノード100とのIPsec通信ができるように、セキュリティアソシエーション900を設定する。

【0207】

以上のように、本実施形態では、例えば、通信を開始する際に認証サーバ、あるいは鍵管理手段を備えた装置等といったグループを構成する機器以外の装置を介さずに、互いに認証可能で安全な通信を行なうことのできるグループを、そのグループを構成する機器が、容易に生成し管理することを実現している。

【0208】

また、グループを生成し管理するために必要な情報を、メモリカードといった記憶媒体を介して各ノードに与えること、および、グループの生成、グループへの参加、および、グループからの離脱の指示を各ノードに与えることを実現している。

【0209】

このように、本実施形態では、サーバなどの特別な機器を設けることなく、また、複数のマスタ鍵などを備えたICカードを用意してグループを構成する機器それぞれに予めセットしておくなどの事前の準備をすることなく、グループを構成する機器間でのみ、容易にIPsec通信可能な環境を構築できる。

【0210】

また、本実施形態では、一つのノードに、グループ内のノードのみ利用できるアプリケーションとグループ外のノードも利用できるアプリケーションとが実装されている場合も容易にそれぞれのアクセス制御を実現できる。

【0 2 1 1】

なお、本実施形態では、グループ生成、加入、離脱時の指示を行なう際に利用する記憶媒体としてメモリカードを例にあげ、説明したが、利用する記憶媒体はこれに限られない。可搬型の記憶媒体であり、各ノードがそのインタフェースを備えていれば、どのような記憶媒体であってもよい。

【0 2 1 2】

また、本実施形態では、I P s e c 通信を行うために必要な情報の授受を記憶媒体で行なうといった設定としたが、これに限られない。例えば、各ノードに入力装置を備え、ユーザが入力するようにしてもよい。

【0 2 1 3】

さらに、グループからの離脱処理を開始するきっかけとして、空のメモリカードの入力を例にあげ説明したが、これに限られない。例えば、各ノードがリセットボタンを備え、ユーザがそのリセットボタンを介して離脱処理を開始する指示を与えるようにしてもよい。

【0 2 1 4】

また、L E D を備えることにより、利用者に対しグループ生成、加入処理の終了を通知する事を実現している。通知のための機能も、これに限られない。

【0 2 1 5】

なお、本発明は上記の実施形態に限定されるものではなく、その要旨の範囲内で様々な変形が可能である。

【0 2 1 6】

例えば、上記の実施形態では、宅内のネットワークを例にとり説明したが、本発明はこれに限定されない。本発明は、互いに認証を必要とする様々なネットワークシステムに広く適用できる。

【0 2 1 7】

【発明の効果】

本実施形態においては、特別に認証サーバまたは鍵管理手段を備えた装置を保有しなくても、グループを構成する機器間で、互いにグループ構成機器であることを認証し、安全な通信を実現するグループを容易に生成し、管理することができる。

【0 2 1 8】

また、機器がグループ内の機器にのみ提供するアプリケーションとグループ外の機器に提供するアプリケーションとを有する場合、そのアクセス制御を簡単な構成にて行なうことができる。

【図面の簡単な説明】

【図 1】 本発明を適用した実施形態のシステム構成を示す図である

【図 2】 本実施形態におけるノードのハードウェア構成を示す図である。

【図 3】 本実施形態におけるノードにおけるソフトウェア構成を示す図である。

【図 4】 グループ通信に用いる A H ヘッド付きの I P パケットの構成を示す図である。

【図 5】 グループ通信に用いる E S P ヘッド付きの I P パケットの構成を示す図である。

【図 6】 本実施形態におけるグループ管理処理部の機能構成を示す図である。

【図 7】 本実施形態におけるグループ制御 I P パケットのデータ部の構成の一例を示す図である。

【図 8】 グループ管理テーブルの構成の一例を示す図である。

【図 9】 アクセス制御対象アプリケーション管理テーブルの構成の一例を示す図である。

【図 1 0】 グループメンバ管理テーブルの構成の一例を示す図である。

【図 1 1】 セキュリティアソシエーションとして設定する情報構成の一例を示す図である。

【図 1 2】 グループ管理処理の処理手順を示す図である。

【図 1 3】 グループ生成処理の処理手順を示す図である。

【図 1 4】 グループ参加処理の処理手順を示す図である。

【図 1 5】 グループ内への新メンバ通知処理の処理手順を示す図である。

【図 16】 グループ離脱処理の処理手順を示す図である。

【図 17】 グループ制御 IP パケット受信処理の処理手順を示す図である。

【図 18】 IP パケット受信時の IP 受信部の処理手順を示す図である。

【図 19】 IP パケット受信時の受信アクセス制御部の処理手順を示す図である。

。

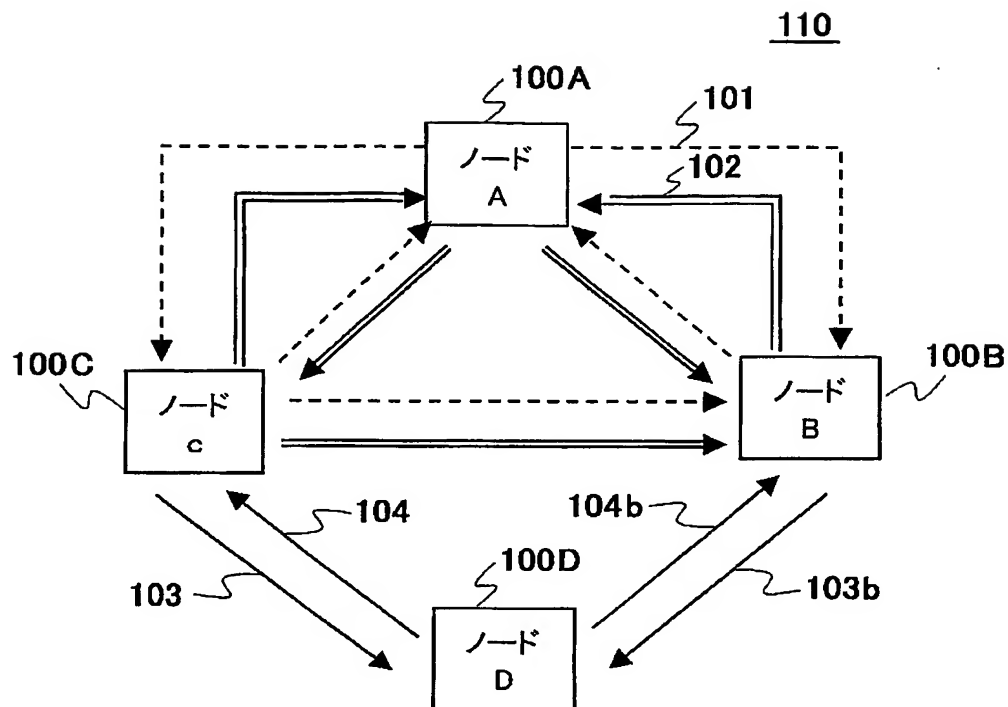
【符号の説明】

100…ノード、301…アプリケーション、302…グループ管理処理部、308…アクセスポリシデータベース、309…SAデータベース、314…IP 受信部、304…IP 送信部、312…IPsec 受信処理部、316…受信アクセス制御部、600…グループ管理テーブル、700…アクセス制御対象アプリケーション管理テーブル、800…グループメンバ管理テーブル、900…セキュリティアソシエーション、3100…制御部、3200…グループ生成処理部、3300…グループ参加処理部、3400…グループ離脱処理部、3500…グループ情報更新処理部、3600…グループ制御 IP パケット受信処理部

【書類名】 図面

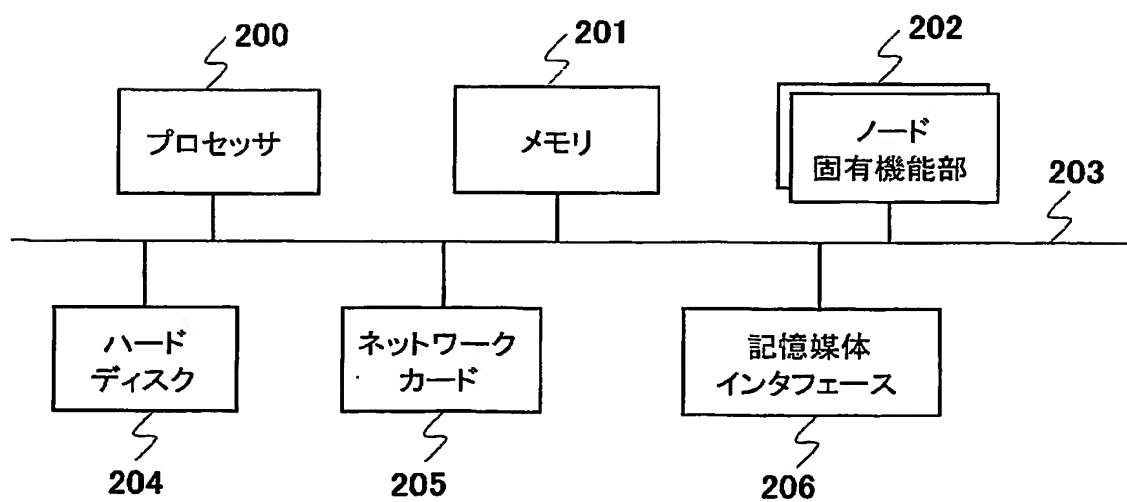
【図 1】

図 1



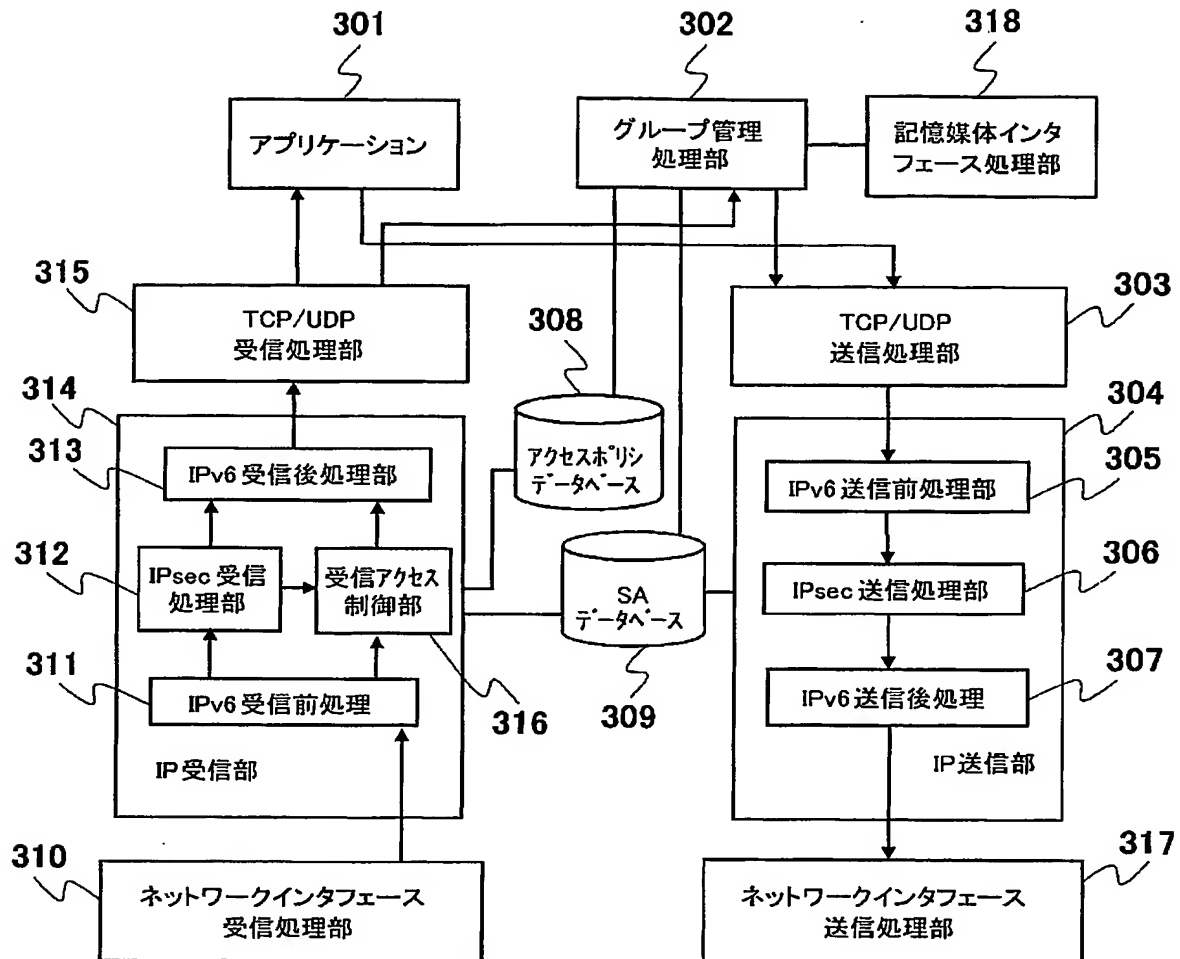
【図 2】

図 2



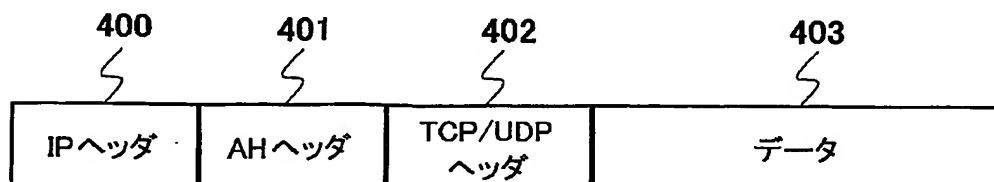
【図 3】

図3



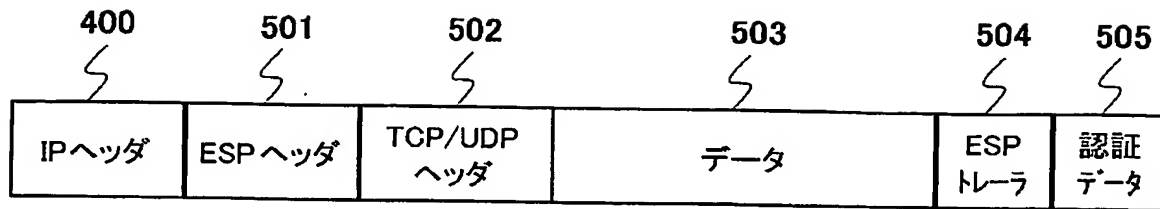
【図 4】

図4



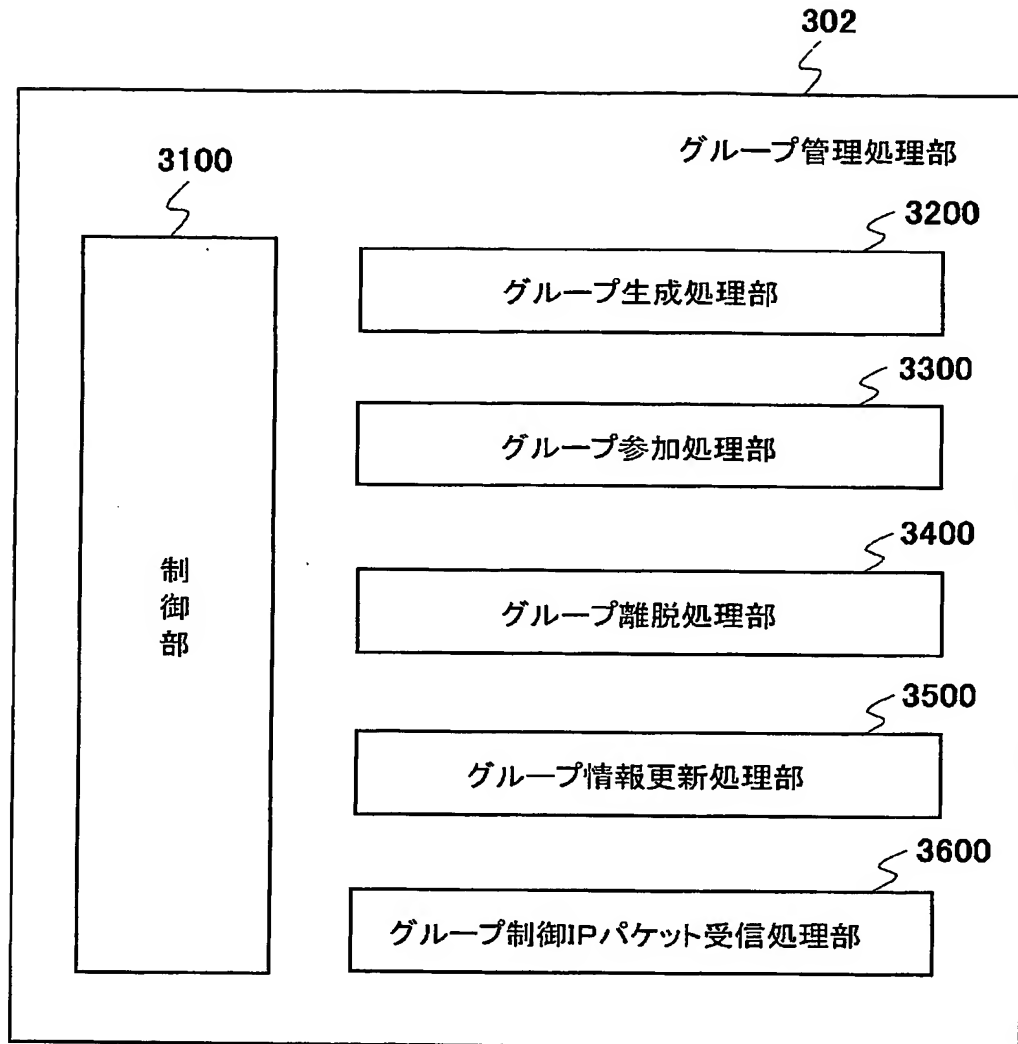
【図 5】

図5



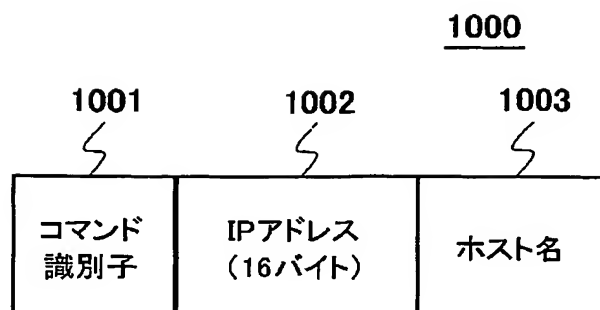
【図 6】

図 6



【図 7】

図 7



【図 8】

図 8

グループ管理テーブル

⚡ 600

グループ識別子	601
グループ鍵	602
鍵有効期限	603
IPsec 種別(認証 / 暗号)	604
アルゴリズム	605
ホスト名 1	606A
⋮	
ホスト名 n	606B

【図 9】

図9

アクセス制御対象アプリケーション管理テーブル

700

ポート番号	701
1024 ~	701A
21	701B
⋮	

【図 10】

図10

グループメンバ管理テーブル 800

801 802 803

801 ⚡	802 ⚡	803 ⚡
ホスト名	IPアドレス	有効期限
ノードA	FE 80 :: 68 12 54 FE 35 01	× × × ×
⋮	⋮	⋮

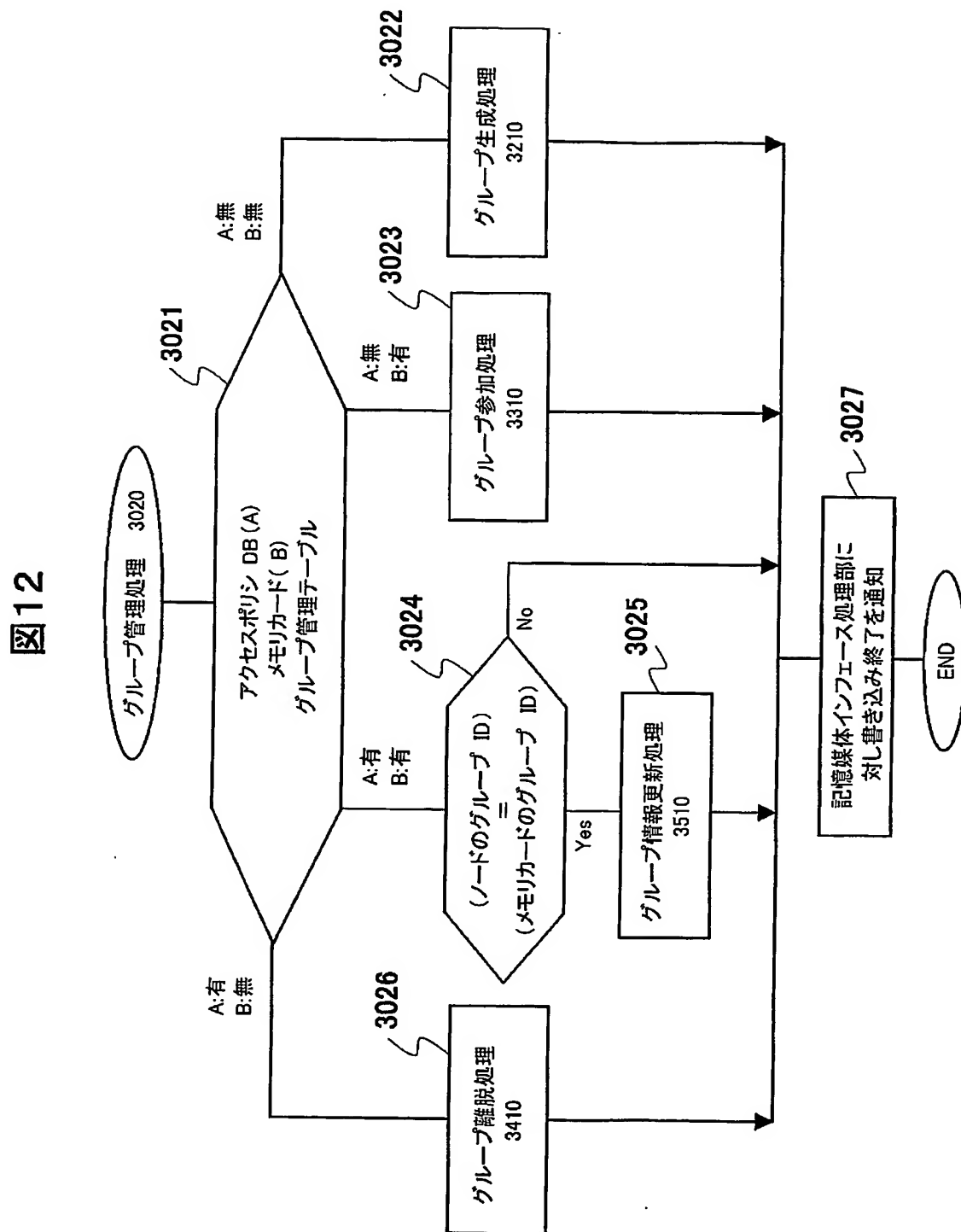
【図 1 1】

図 1 1

セキュリティアソシエーション 900

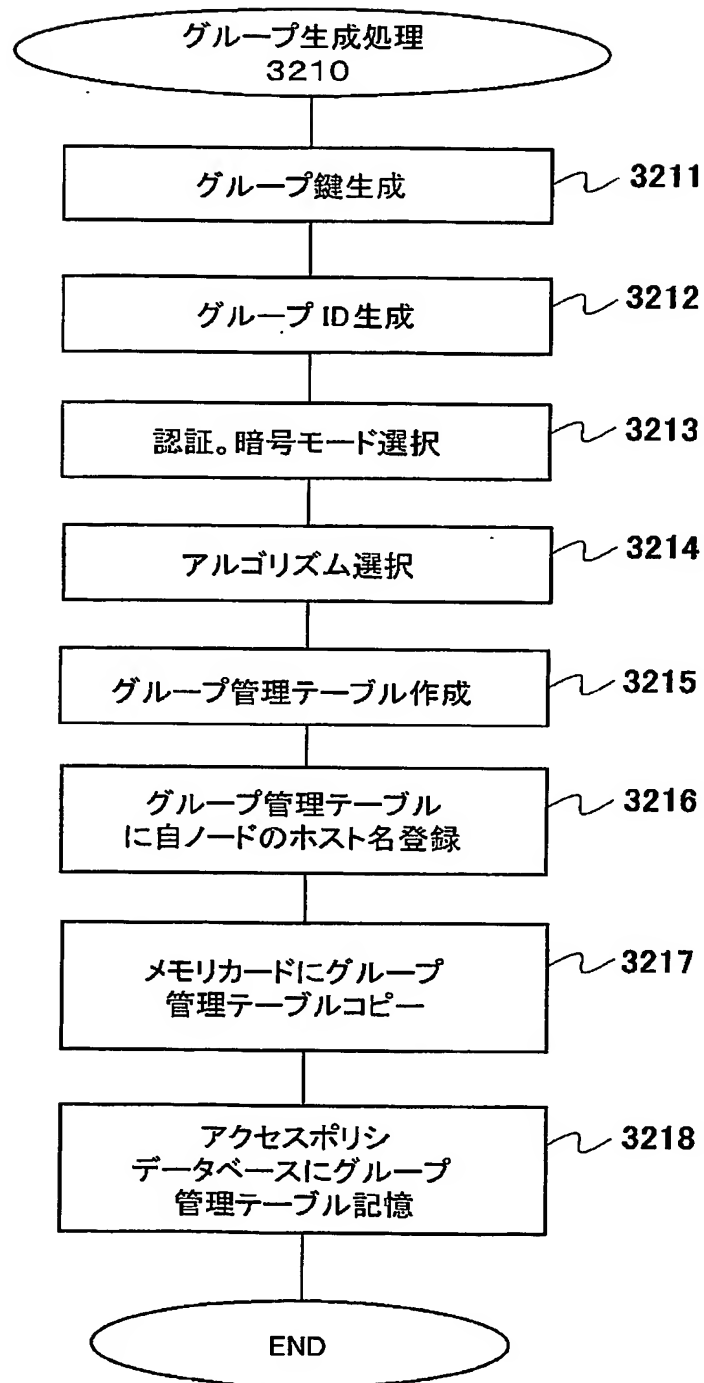
SPI	グループ識別子
送信元 IP アドレス	FE 80 :: 68 12 54 FE 35 01
送信先 IP アドレス	FE 80 :: 68 12 54 FE 35 02
プロトコル	AH
モード	トランスポート
暗号アルゴリズム	——
暗号鍵	——
認証アルゴリズム	SHA-1
認証鍵	グループ管理テーブル上のグループ鍵
有効期限	in 7 days

【図 12】



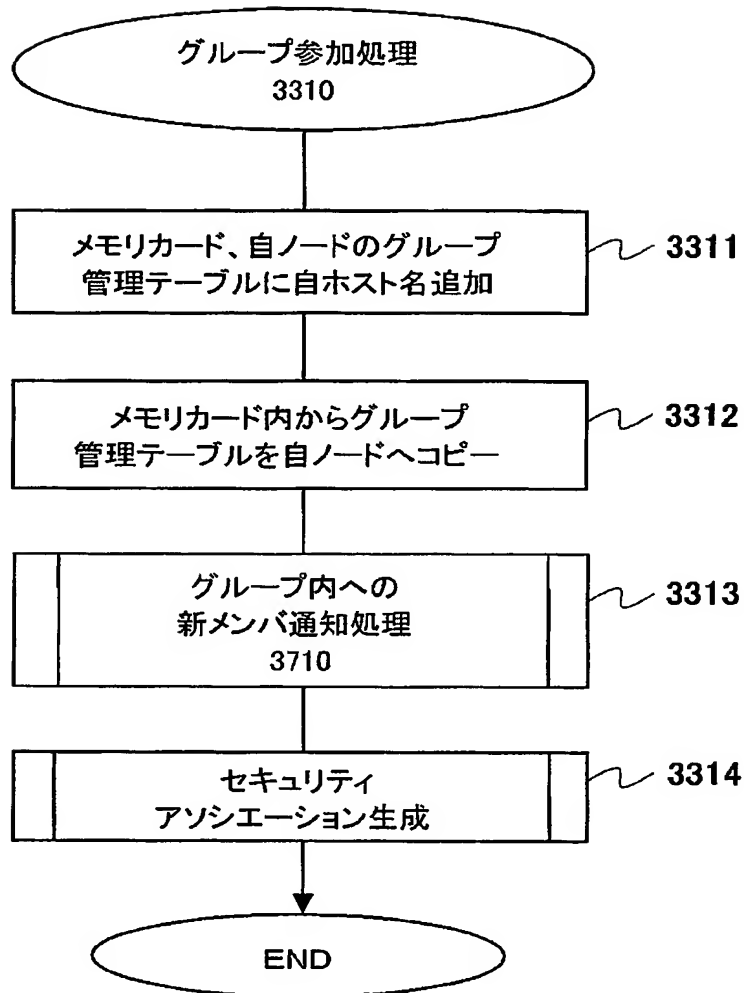
【図 13】

図 13



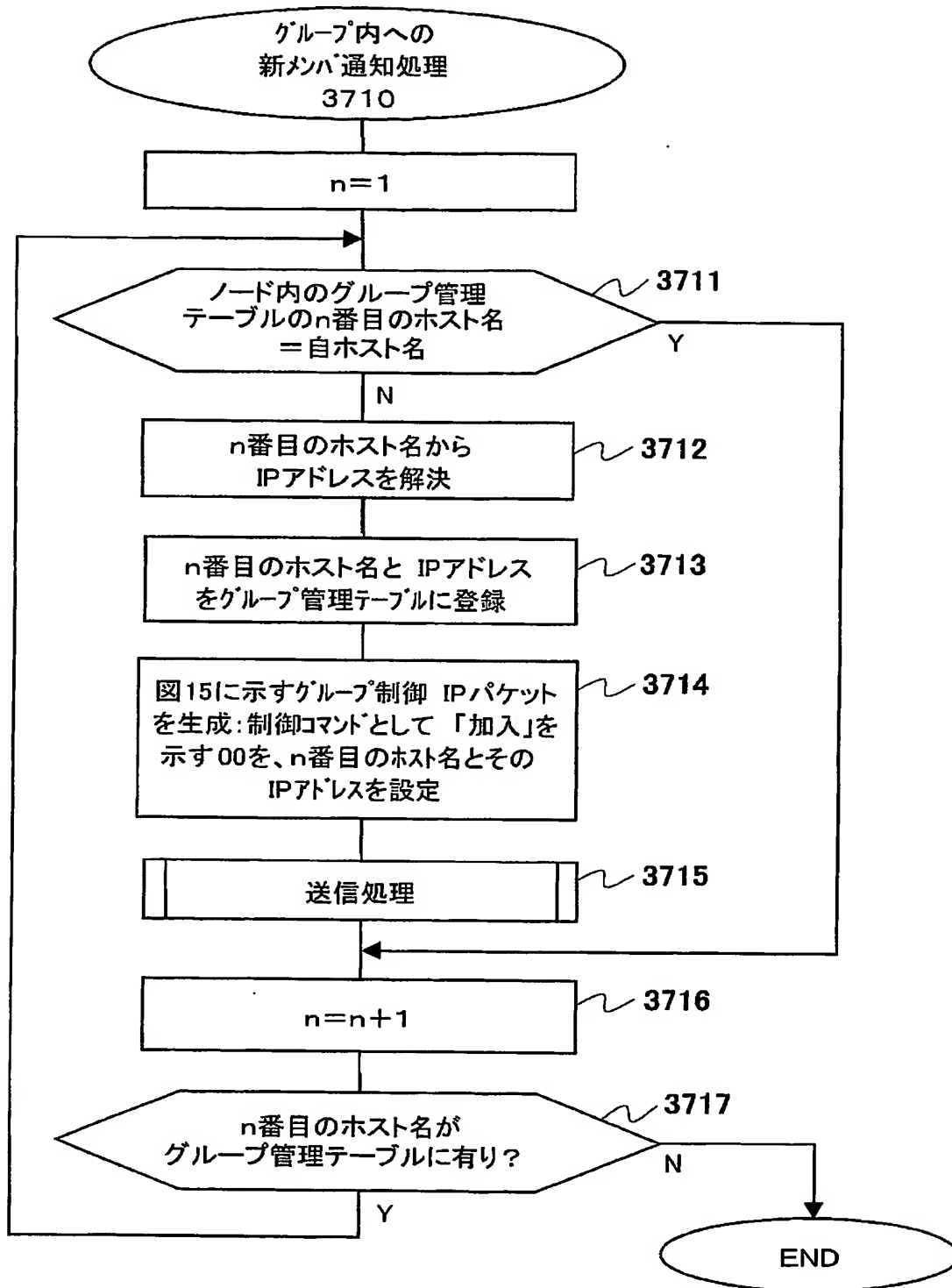
【図 14】

図 14



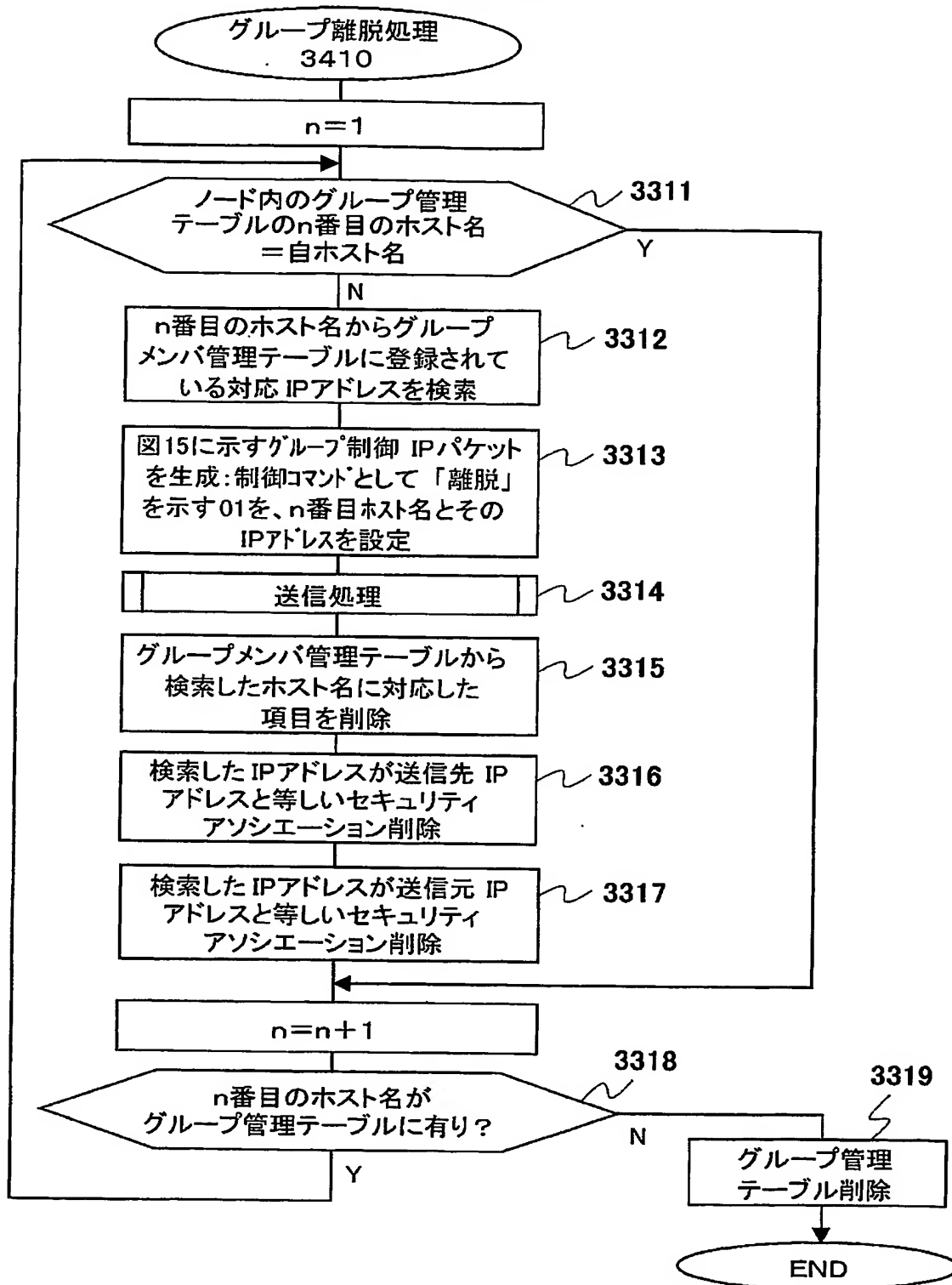
【図 15】

図15



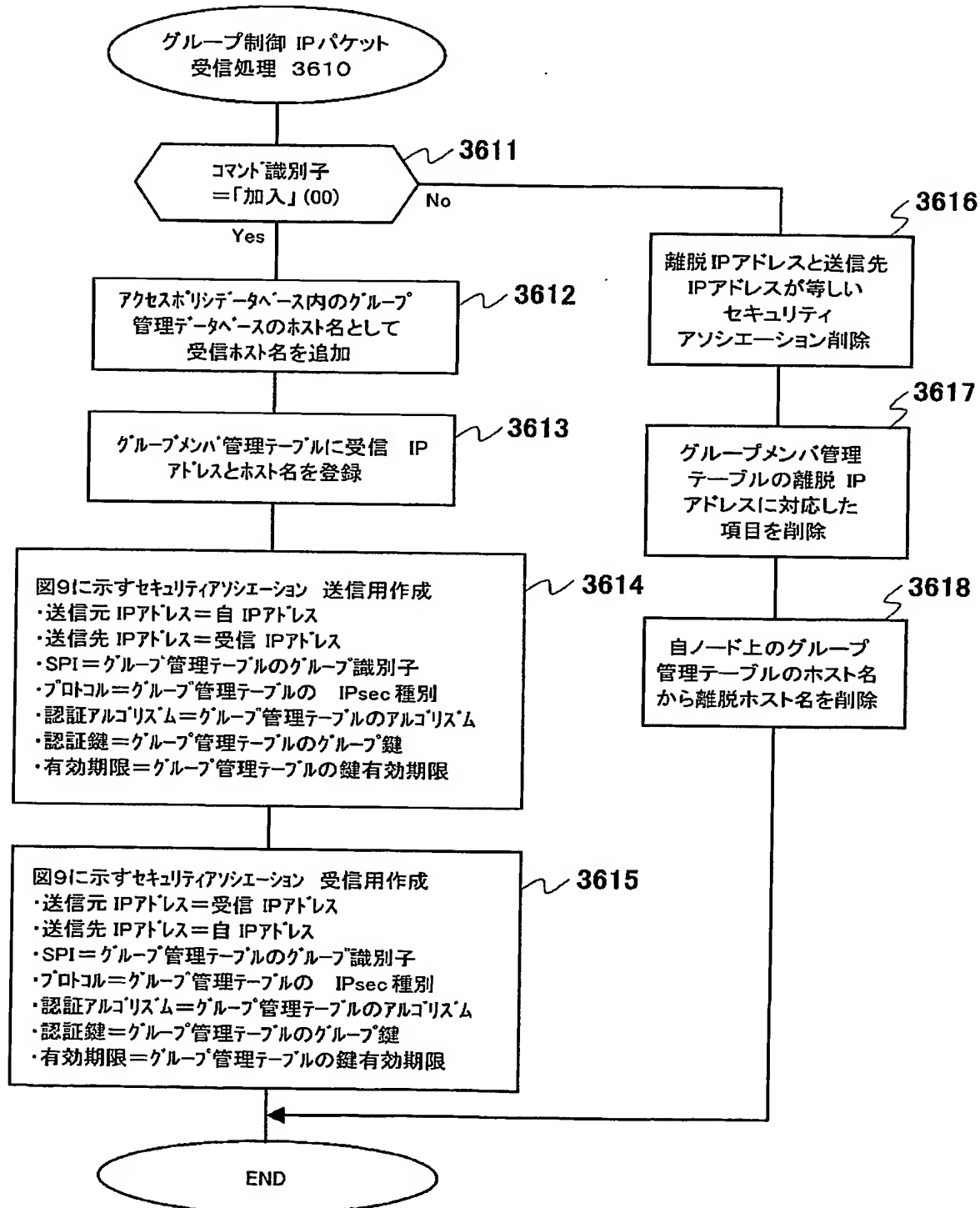
【図 16】

図16



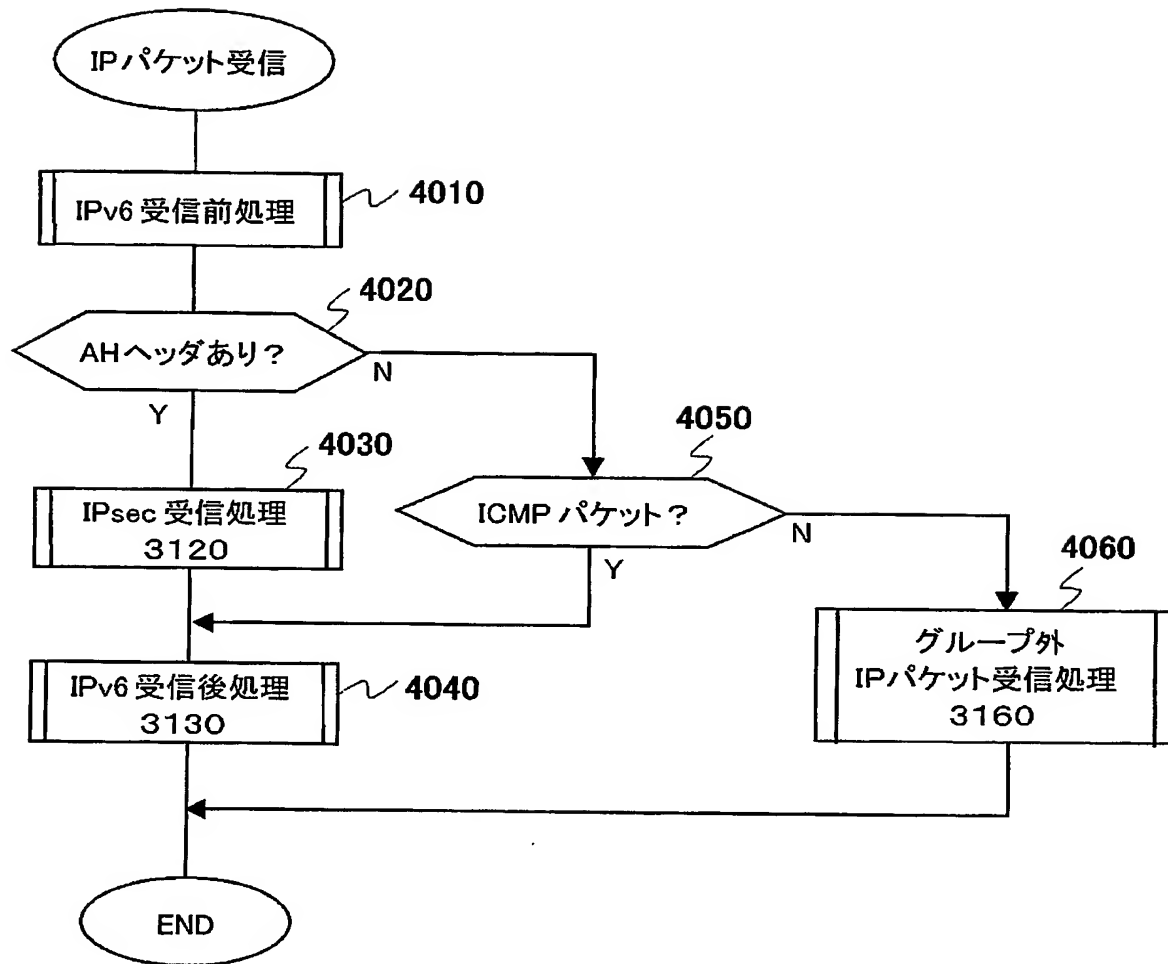
【図 17】

図17



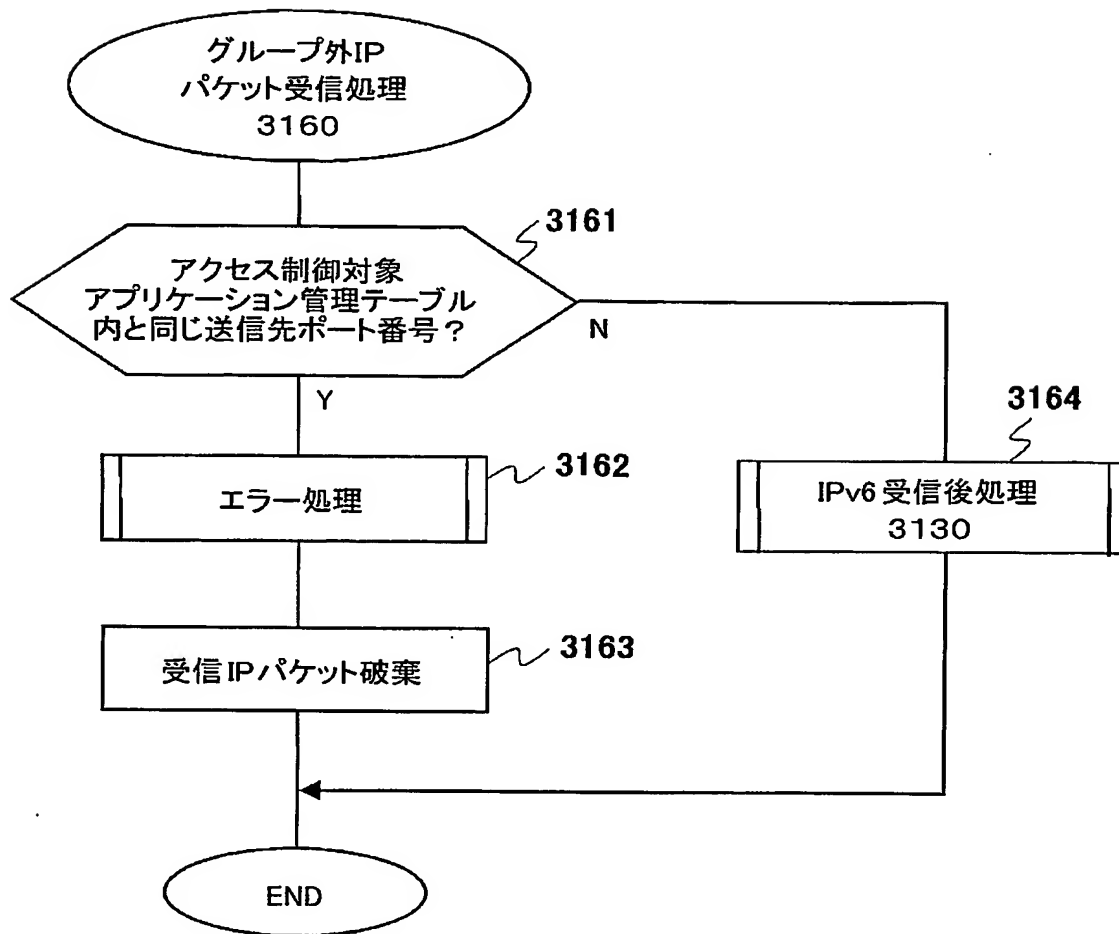
【図18】

図18



【図19】

図19



【書類名】 要約書

【要約】

【課題】

利用者が認めた機器でグループを構成し、グループに属する機器間の安全な通信を実現する。

【解決手段】

グループ管理処理部 3 0 2 にて、グループ内の暗号通信に用いる暗号化鍵を作成し、暗号通信に必要な情報とともに自身の記憶部と記録媒体とに格納する。その記録媒体を用いて、暗号通信に必要な情報を受けとった機器は、その情報を用いて既にグループに属している他の機器に自身と暗号通信を行なうために必要な情報を送信する。

グループから離脱する場合は、自身が保有している暗号通信を行なうための情報を削除するとともに、他の機器に自身の離脱を通知し、通知を受けた機器内の離脱する機器に関する情報を削除してもらう。

【選択図】 図 3

特願 2 0 0 2 - 3 7 5 1 2 3

ページ : 1/E

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 1 0 8]

1. 変更年月日

1 9 9 0 年 8 月 3 1 日

[変更理由]

新規登録

住 所

東京都千代田区神田駿河台 4 丁目 6 番地

氏 名

株式会社日立製作所